INTRODUCTION TO GROUP THEORY (MATH 10005)

COURSE NOTES 2014-2015

1. SYMMETRIES

The main idea of group theory is to deal mathematically with the idea of "symmetry". Before even giving the definition of a group, we'll look at several examples of symmetries of objects, so that the formal definition will make more sense when we come to it.

Exactly what we mean by a "symmetry" will vary from example to example, and sometimes there's more than one sensible notion for the same object, so rather than giving a general definition, we'll clarify what we mean in each example, and the common features should become clear.

1.1. **Permutations of a set.** We'll go through this first example in quite some detail.

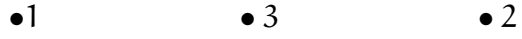
Let X be a set. For example, it might be a set of three elements. Imagine them arranged in a line:

We can rearrange them, putting them in a different order. For example, we could swap the two elements furthest to the right:

This leaves us with exactly the same picture, so we'll regard this as a "symmetry" in this context.

Now let's label the elements so that we can see how the elements have been permuted. We start with:

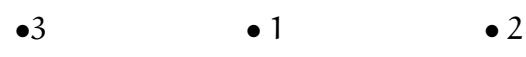
After swapping the two elements 2 and 3, we get:



We can think of this as given by a function $F : X \to X$, where $F(x)$ tells us to which position we have moved element x. So in the example above:

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

Or if we cyclically permuted the elements to the position



then the corresponding function would be

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

as 1 has moved to position 2, 2 to position 3, and 3 to position 1.

[**Note:** We could alternatively think of the function where $F(x)$ tells us which element has moved to position x, in which case, in the last example we'd have $F(1) = 3$, $F(2) = 1$ and $F(3) = 2$. There's nothing wrong with doing this, but note that it gives a different function, and to avoid confusion we'll stick to the first convention.]

If this is to count as a "symmetry" of the original position, then we don't want to move two elements to the same place, or to leave a place unoccupied,

as this gives a different pattern.

Mathematically, in terms of the function F, this is just saying that

(1) $F(x) = F(y) \Rightarrow x = y$ (different elements are sent to different places). I.e., F is an **injective** function.
(2) For every $y \in X$, $y = F(x)$ for some $x \in X$ (every place gets occupied). I.e., F is a **surjective** function.

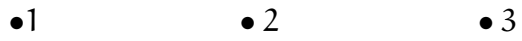
[If X is finite, then these two conditions are equivalent, but if X is infinite then we need both. For example, if $X = \{1, 2, 3, \dots\}$ is the set of positive integers, then the function given by $F(x) = x + 1$ is injective but not surjective, and the function given by $G(x) = x - 1$ if $x > 1$ and $G(1) = 1$ is surjective but not injective.]

In other words, we want F to be a **bijective** function. Recall that this just means a function that is both injective and surjective. Or equivalently, such that there is exactly one element of the domain sent to each element of the codomain. Or equivalently again, a function with an inverse F^{-1}.

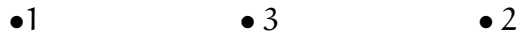
So to make everything precise, let's just **define** a "permutation" of a set X to be a bijective function from X to X.

Let's look in more detail at the permutations of a set $X = \{1, 2, 3\}$ with three elements. It's easy to check that there are just six of these, which we'll denote by E, F, G, H, I and J:

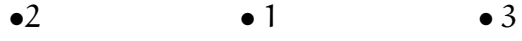
$$E(1) = 1,\ E(2) = 2,\ E(3) = 3$$



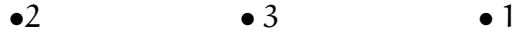
$$F(1) = 1,\ F(2) = 3,\ F(3) = 2$$



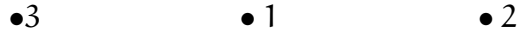
$$G(1) = 2,\ G(2) = 1,\ G(3) = 3$$



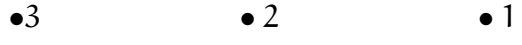
$$H(1) = 3,\ H(2) = 1,\ H(3) = 2$$



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



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



The first of these is rather dull: we don't move anything. Every element is left where it started. We'll call this the **identity** permutation.

Now we can look at what happens when we perform one permutation followed by another. For example, if we do F (swap the two elements furthest to the right) and then G (swap the two elements that are now furthest to the left), then we are just taking the composition $G \circ F$ of the two functions.

This gives $G(F(1)) = G(1) = 2$, $G(F(2)) = G(3) = 3$ and $G(F(3)) = G(2) = 1$. So $G \circ F = I$. Note that when we compose two permutations, we'll always get another permutation (the composition of two bijections is a bijection).

For simplicity, we'll leave out the composition symbol $\circ$ and write GF instead of $G \circ F$.

Let's see what FG is.

$F(G(1)) = F(2) = 3$, $F(G(2)) = F(1) = 1$ and $F(G(3)) = F(3) = 2$, so $FG = H$.

Notice that it makes a difference which order we do F and G: $GF = I$ but $FG = H$.

NOTE: When composing permutations or other symmetries, the order does matter in general. GF will always mean "do F first and then G" as in the notation for functions ($g(f(x))$ is what we get when we apply the function f and then the function g), rather than reading from left to right.

When we come to define groups, we'll think of "composition" as an operation to combine permutations or other kinds of symmetry (if F and G are symmetries of an object, then GF is the symmetry "do F and then G"), much as "multiplication" is an operation to combine numbers. In fact we're using pretty much the same notation: compare GF for permutations with xy for numbers. However, one important difference is that, as we've seen, GF may not be the same as FG, whereas multiplying numbers, we have the commutative law $xy = yx$.

Sticking with the example of permutations of a set X, what other general features can we identify?

(a) We always have the **identity** permutation E, where $E(x) = x$ for every $x \in X$. If D is another permutation, then clearly doing D and then E (or E and then D) is the same as just doing D. In symbols,

$$ED = D = DE.$$

(b) Any permutation D has an inverse D^{-1}, which is also a permutation (D is a bijection, so it has an inverse that is also a bijection). Doing D and then D^{-1} (or vice versa) will give the identity permutation E. In symbols,

$$D^{-1}D = E = DD^{-1}.$$

[In the example above, where $X = \{1, 2, 3\}$, you can check that $E^{-1} = E$, $F^{-1} = F$, $G^{-1} = G$, $H^{-1} = I$, $I^{-1} = H$ and $J^{-1} = J$.

(c) If B, C and D are permutations, then $B(CD)$ means "do D and then C, giving a permutation CD, and then do B".

$(BC)D$ means "do D, and then do the permutation you get by doing C and then B".

But both of these are just applying D, then C, and then D, so clearly give the same permutation. So where we put the brackets makes no difference (unlike the order in which we perform the permutations, which does make a

difference), and we get the associative law

$$B(CD) = (BC)D.$$

These three properties, which are almost obvious in this example, will be at the heart of our abstract definition of a group.

1.2. **Symmetries of polygons.** Consider a regular n-sided polygon (for example, if $n = 3$ an equilateral triangle, or if $n = 4$ a square). Examples of symmetries are

(1) A rotation through an angle of $2\pi/n$ (an nth of a revolution).
(2) A reflection in a line that goes through the centre of the polygon and one of its vertices.

There are many ways to make precise what we mean by a symmetry. For example, considering the polygon as a subset X of $\mathbb{R}^2$, we could look at bijections $F : X \to X$ that preserve distance: i.e., such that the distance between $F(x)$ and $F(y)$ is the same as the distance between x and y. It's not hard to see that this implies that f must send vertices to vertices, and moreover must send **adjacent** vertices to adjacent vertices. To keep things simple, we'll use this as our **definition** of a symmetry:

Definition 1.1. A **symmetry** of a regular n-sided polygon is a permutation F of the set of n vertices that preserves adjacency: i.e., so that for vertices u and v, u and v are adjacent if and only if $F(u)$ and $F(v)$ are adjacent.

Note that for $n = 3$, every pair of vertices is adjacent, so in that case **every** permutation of the vertices is a symmetry, and so we are just looking at permutations of a set of three elements as in the last section.

In the case $n = 4$, we have a square. Let's label the vertices as follows:

$$\begin{array}{ccc} 2 & \leftrightarrow & 1 \\ \updownarrow & & \updownarrow \\ 3 & \leftrightarrow & 4 \end{array}$$

Then, for example,

$$\begin{array}{ccc} 1 & \leftrightarrow & 4 \\ \updownarrow & & \updownarrow \\ 2 & \leftrightarrow & 3 \end{array}$$

is what we get when we rotate anticlockwise through an angle of $\pi/2$ (let's call this symmetry F), and

$$\begin{array}{ccc} 4 & \leftrightarrow & 1 \\ \updownarrow & & \updownarrow \\ 3 & \leftrightarrow & 2 \end{array}$$

is what we get if we reflect in the line of symmetry going from top right to bottom left (let's call this G). But

$$\begin{array}{ccc} 1 & \leftrightarrow & 2 \\ \updownarrow & & \updownarrow \\ 3 & \leftrightarrow & 4 \end{array}$$

does not represent a symmetry, as vertices 2 and 3 have not remained adjacent.

The identity permutation E is also a symmetry, and the inverse of a symmetry is a symmetry. In fact, the three features (a) to (c) we noted for permutations also apply here, and for exacly the same reasons.

Let's look at what happens when we compose the symmetries F and G.

If we do F, then G, to calculate GF, we get

$$\begin{array}{ccc} 3 & \leftrightarrow & 4 \\ \updownarrow & & \updownarrow \\ 2 & \leftrightarrow & 1 \end{array}$$

which is a reflection in the horizontal line of symmetry.

If we do G, then F, to calculate FG, we get

$$\begin{array}{ccc} 1 & \leftrightarrow & 2 \\ \updownarrow & & \updownarrow \\ 4 & \leftrightarrow & 3 \end{array}$$

which is a reflection in the vertical line of symmetry.

Note that again the order matters: $FG \neq GF$.

1.3. **Symmetries of a circle.** We can look at bijections from a circle to itself that preserve distances between points. It's not too hard to see that these symmetries are either rotations (through an arbitrary angle) or reflections (in an arbitrary line through the centre).

Again, if F and G are symmetries, then usually $FG \neq GF$.

1.4. **Symmetries of a cube.** We can look at the eight vertices of a cube, and define a symmetry to be a permutation of the set of vertices that preserves adjacency (as we did with a polygon). There are 48 symmetries: most are either rotations or reflections, but there is also the symmetry that takes each vertex to the opposite vertex.

1.5. **Rubik's Cube.** A Rubik's cube has 54 coloured stickers (9 on each face), and we could define a "symmetry" to be a permutation of the stickers that we can achieve by repeatedly turning faces (as one does with a Rubik's cube). It turns out that there are $43,252,003,274,489,856,000$ symmetries. Again we can compose symmetries (do one sequence of moves and then another), and every symmetry has an inverse symmetry.

2. Definition of a group and first examples

We want to formalize the structure of symmetries of the kind we looked at in Section 1. When we look at permutations of a set, for example, we have the set of permutations, and we also have a way of combining two permutations, by composition, to get a third.

We can formalize this as follows.

Definition 2.1. A **binary operation** on a set G is a function

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

Remember that $G \times G$ is just the set

$$\{(x, y) : x, y \in G\}$$

of ordered pairs of elements of G, so this just means that we have a function that gives a value $\star(x, y)$ in G for every pair of elements x, y of G. The word "binary" refers to the fact that the operation takes *two* inputs, x and y.

We'll usually write $x \star y$ instead of $\star(x, y)$.

Examples:

(1) Composition $\circ$ is a binary operation on the set G of permutations of a set X.
(2) Addition $+$ is a binary operation on the set $\mathbb{R}$ of real numbers (or on the set $\mathbb{Z}$ of integers, or the set $\mathbb{Q}$ of rational numbers).
(3) Multiplication and subtraction are also binary operations on $\mathbb{R}$.

Note that in the definition of a binary operation, the function $\star$ maps to G, so if we have a definition of $x \star y$ so that $x \star y$ is not always in G, then this is not a binary operation on G (we say that G is not **closed** under $\star$). Also, the domain of $\star$ is $G \times G$, so $x \star y$ needs to be defined for **all** pairs of elements x, y.

Non-examples:

(1) Subtraction is not a binary operation on the set $\mathbb{N}$ of natural numbers, since, for example, $4 - 7 = -3$ is not a natural number. So $\mathbb{N}$ is not closed under subtraction.
(2) Division is not a binary operation on the set $\mathbb{R}$ of real numbers, since x/y is not defined when $y = 0$. (But division is a binary operation on the set $\mathbb{R} \setminus \{0\}$ of **non-zero** real numbers.

For a general binary operation, the order of the elements x, y matters: $x \star y$ is not necessarily equal to $y \star x$.

Definition 2.2. A binary operation $\star$ on a set G is called **commutative** if

$$x \star y = y \star x$$

for all elements $x, y \in G$.

Examples:

(1) Addition and multiplication are commutative binary operations on $\mathbb{R}$.
(2) Subtraction is not commutative on $\mathbb{R}$ since, for example, $2-1=1$ but $1-2=-1$.
(3) Composition is not a commutative operation on the set of permutations of the set $\{1,2,3\}$.

Bearing in mind the example of permutations of a set X, and the properties that we noted about composing permutations, we'll now define a group.

Definition 2.3. A **group** $(G,\star)$ is a set G together with a binary operation $\star : G\times G\to G$ satisfying the following properties (or "axioms").

(1) (Associativity) For all $x,y,z\in G$,
$$(x\star y)\star z = x\star(y\star z).$$
(2) (Existence of an identity element) There is an element $e\in G$ (called the **identity** element of the group) such that, for every $x\in G$,
$$x\star e = x = e\star x.$$
(3) (Existence of inverses) For every $x\in G$, there is an element $x^{-1}\in G$ (called the **inverse** of x) such that
$$x\star x^{-1} = e = x^{-1}\star x.$$

Strictly speaking, the group consists of both the set G **and** the operation $\star$, but we'll often talk about "the group G" if it's clear what operation we mean, or say "G is a group under the operation $\star$". But the same set G can have several different group operations, so we need to be careful.

Example 2.1. If X is a set, $S(X)$ is the set of all permutations of X (i.e., bijective functions $X\to X$), and $f\circ g$ is the composition of bijections f and g, then $(S(X),\circ)$ is a group.

Note that in this example, there are two sets involved (X and the set $S(X)$ of permutations). It is the set $S(X)$ that is the group, not X (we haven't defined a binary operation on X).

Example 2.2. The set of all symmetries of a regular n-sided polygon is a group under composition, as is the set of all symmetries of a cube, or a Rubik's cube.

These examples, and similar ones, of **symmetry groups**, are the motiation for the definition of a group, but there are some other familiar examples of sets of numbers with arithmetical operations that fit the definition.

Example 2.3. $(\mathbb{R},+)$ is a group. [Addition is associative, the identity element is 0, and the inverse of x is $-x$.]

Example 2.4. $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are groups.

Example 2.5. The set of positive integers is **not** a group under addition, since it doesn't have an identity element. The set of non-negative integers is still not a group, as although it has the identity element 0, no integer $n > 0$ has an inverse (since $-n$ is not a non-negative integer.

Example 2.6. The set $\mathbb{R} \setminus \{0\}$ of non-zero real numbers is a group under multiplication. [Multiplication is associative, the identity element is 1, and the inverse of x is $\frac{1}{x}$.]

Example 2.7. $(\mathbb{R}, \times)$ is **not** a group, since 0 does not have an inverse.

Example 2.8. $\mathbb{R}$ is not a group under subtraction, since associativity fails: $(x-y)-z = x-y-z$, but $x-(y-z) = x-y+z$, and so these are different whenever $z \neq 0$.

Matrices are another source of examples.

Example 2.9. Let $M_n(\mathbb{R})$ be the set of $n \times n$ matrices with real entries. Then $M_n(\mathbb{R})$ is a group under addition.

Example 2.10. $M_n(\mathbb{R})$ is not a group under matrix multiplication, since not every matrix has an inverse. However, the set of *invertible* $n \times n$ matrices is a group under multiplication.

We've stressed that $x \star y$ and $y \star x$ are typically different in symmetry groups. But in the examples coming from addition and multiplication of integers, they are the same.

Definition 2.4. A group $(G, \star)$ is called **abelian** if

$$x \star y = y \star x$$

for all $x, y \in G$.

The word "abelian" is derived from the name of the Norwegian mathematician Niels Henrik **Abel**.

Even in a non-abelian group, $x \star y = y \star x$ may hold for *some* elements x and y (in which case we say that x and y **commute**, but for the group to be abelian it must hold for *all* elements.

Examples:

(1) The group $S(X)$ of permutations of a set X is non-abelian if X has at least three elements, since if $x, y, z \in X$ are three distinct elements, f is the permutation that swaps x and y (and fixing all other elements), g is the permutation that swaps y and z, then $f \circ g \neq g \circ f$.

(2) More generally, symmetry groups are typically non-abelian (although sometimes they are). In particular, the symmetry group of a regular n-sided polygon (where $n \geq 3$) is non-abelian.

(3) $(\mathbb{R}, +)$ is abelian, since $x + y = y + x$ for all real numbers x, y.
(4) $(\mathbb{R} \setminus \{0\}, \times)$ is abelian.
(5) $M_n(\mathbb{R})$ is an abelian group under matrix addition.
(6) If $n \geq 2$, then the set of invertible $n \times n$ real matrices is a non-abelian group under matrix multiplication, since for example

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

but

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Often, especially when we're dealing with abstract properties of general groups, we'll simplify the notation by writing xy instead of $x \star y$, as though we're multiplying. In this case we'll say, for example, "Let G be a **multiplicatively-written** group". Note that this is purely a matter of the notation we use for the group operation: **any** group can be "multiplicatively-written" if we choose to use that notation, so if we prove anything about a general multiplicatively-written group, it will apply to all groups, no matter what the group operation is.

Of course, if we're looking at something like the group of real numbers under addition, it would be incredibly confusing to write this multiplicatively, so in cases like that, where multiplication already has some other meaning, or where there's already another standard notation for the group operation, we'll tend not to use multiplicative notation.

Notice that in a multiplicatively-written group, the associativity axiom says

$$(xy)z = x(yz),$$

and from this it follows easily (by induction, for example) that any product such as $wxyz$ has a unique meaning: we could bracket it as $(wx)(yz)$ or $(w(xy))z$ or $w((xy)z)$ or any of the other possible ways, and because of associativity they would all give the same element.

Recommendation: Because examples such as $(\mathbb{R}, +)$ are abelian, which is not typical for a group, it can be misleading to try to get your intuition for how groups work from examples like this. A much better simple example to use is the group of permutations of $\{1, 2, 3\}$ or, if you like thinking more geometrically, the group of symmetries of an equilateral triangle (actually, since all vertices of a triangle are adjacent, this is really just the same as the group of permutations of the set of vertices), or of a square.

3. Elementary consequences of the definition

Throughout this section, G will be a multiplicatively written group. Remember that being "multiplicatively written" is purely a matter of notation, so everything will apply to any group.

A familiar idea from elementary algebra is that if you have some equation (involving real numbers, say) such as

$$ax = bx$$

then you can "cancel" the x (so long as $x \neq 0$) to deduce that $a = b$.

A similar principle applies in a group, because of the fact that elements all have inverses, with one complication caused by the fact that the group operation may not be commutative.

The idea is that we can "divide" by x by multiplying by x^{-1}, although multiplying on the left and on the right are in general different, so we need to decide which is appropriate.

Proposition 3.1 (Right cancellation)**.** *Let* a, b, x *be elements of a multiplicatively written group* G*. If* $ax = bx$*, then* $a = b$*.*

Proof. Multiply on the right by x^{-1}:

$$ax = bx \Rightarrow (ax)x^{-1} = (bx)x^{-1} \Rightarrow a(xx^{-1}) = b(xx^{-1}) \Rightarrow ae = be \Rightarrow a = b.$$

□

Proposition 3.2 (Left cancellation)**.** *Let* a, b, x *be elements of a multiplicatively written group* G*. If* $xa = xb$*, then* $a = b$*.*

Proof. Multiply on the left by x^{-1}:

$$xa = xb \Rightarrow x^{-1}(xa) = x^{-1}(xb) \Rightarrow (x^{-1}x)a = (x^{-1}x)b \Rightarrow ea = eb \Rightarrow a = b.$$

□

[**WARNING:** If $ax = xb$, then in a non-abelian group it is not necessarily true that $a = b$, since to "cancel" x from both sides of the equation we need to multiply the left hand side by x^{-1} on the *right*, but multiply the right hand side by x^{-1} on the *left*, and these are different operations.]

This simple principle has some nice consequences that make studying groups easier. One is that the defining property of identity element e is enough to identify it: no other element has the same property.

Proposition 3.3 (Uniqueness of the identity)**.** *Let* a, x *be elements of a multiplicatively written group. If* $ax = a$ *then* $x = e$*.*

Proof. If $ax = a$ then $ax = ae$. By "left cancellation", we can cancel a to deduce $x = e$. □

Similarly, using "right cancellation", if $xa = a$ then $x = e$.

A similar proof shows that an element of a group can only have one inverse.

Proposition 3.4 (Uniqueness of inverses)**.** *Let x, y be elements of a multiplicatively written group. If $xy = e$ then $x = y^{-1}$ and $y = x^{-1}$.*

Proof. If $xy = e$ then $xy = xx^{-1}$, and so, by left cancellation $y = x^{-1}$. Similarly, if $xy = e$ then $xy = y^{-1}y$, and so by right cancellation $x = y^{-1}$. □

This means that, to prove that one element x of a group is the inverse of another element y, we just need to check that their product (either way round: xy or yx) is equal to the identity. Here are some examples of useful facts that we can prove like this:

Proposition 3.5. *Let x be an element of a multiplicatively written group. Then the inverse of x^{-1} is x: $(x^{-1})^{-1} = x$.*

Proof. By uniqueness of inverses, we just need to check that $xx^{-1} = e$, which is true. □

Proposition 3.6. *Let x, y be elements of a multiplicatively writtten group. Then the inverse of xy is $(xy)^{-1} = y^{-1}x^{-1}$.*

Proof. By uniqueness of inverses, we just need to check that $(xy)(y^{-1}x^{-1}) = e$. But

$$(xy)(y^{-1}x^{-1}) = ((xy)y^{-1})x^{-1} = (x(yy^{-1}))x^{-1} = (xe)x^{-1} = xx^{-1} = e.$$

□

Make sure you understand how each step of the previous proof follows from the definition of a group, and in particular how I have used the associative property. In future I will often be less explicit about this, leaving out brackets.

WARNING: Note that in a non-abelian group it is **not** in general true that $(xy)^{-1} = x^{-1}y^{-1}$, since $x^{-1}y^{-1} \neq y^{-1}x^{-1}$ in general. The fact that we need to reverse the order like this may well be familiar to you from taking inverses of matrices.

The cancellation properties have a nice interpretation in terms of the "multiplication table" of a group. Let G be a group with a finite number of elements: its multiplication table (often also called the **Cayley table** after the 19th century British mathematician Arthur Cayley) has one row and one column for each element of the group, and the entry in column x and row y is the product xy. So the table displays the group operation.

Then left cancellation just says that all the entries in each column are different: if two entries xy and xz in column x are the same, then $xy = xz$ and so $y = z$. Similarly the right cancellation property says that all the entries in each row are different. This can be a useful method for deducing information about a group from a partial multiplication table.

Next, some notation. If $x \in G$, then we'll write x^2 for the product xx of x with itself, x^3 for the product $x(x^2)$ (which is the same as $(x^2)x$ by associativity), and so on.

Note that for $n = -1$ we also have a meaning for x^n, since x^{-1} is notation we use for the inverse of x.

Let's extend this even further by defining x^{-n} to be $(x^n)^{-1}$ if $n > 0$ (which gives us a meaning for x^n for any non-zero integer n, positive or negative) and defining x^0 to be the identity element e (so that we now have a meaning for x^n for *every* integer n. We'll call x^n the n**th power** of x.

Remark 3.1. If G is the group of non-zero real numbers under multiplication, then this meaning of x^n is the same as the meaning you're used to.

To justify why this is a sensible notation, we'll see what happens when we multiply powers. First:

Lemma 3.7. *If $n > 0$ then $x^{-n} = (x^{-1})^n$.*

Proof. By definition, $x^{-n} = (x^n)^{-1}$. To prove this is the same as $(x^{-1})^n$ we just have to show $(x^{-1})^n x^n = e$, by uniqueness of inverses. But

$$(x^{-1})^n x^n = x^{-1} \dots x^{-1} x^{-1} x x \dots x = x^{-1} \dots x^{-1} e x \dots x = x^{-1} \dots x^{-1} x \dots x = \dots = e,$$

cancelling each x^{-1} with an x. □

Proposition 3.8. *If x is an element of a multiplicatively written group G, and m and n are integers, then*

$$(x^m)(x^n) = x^{m+n}.$$

Proof. We'll first prove this (by induction) when $m \geq 0$. It is true when $m = 0$ since

$$(x^0)(x^n) = e(x^n) = x^n.$$

Suppose it is true for $m = k - 1$. Then

$$(x^k)(x^n) = \left(x(x^{k-1})\right)(x^n) = x\left((x^{k-1}(x^n)\right) = x(x^{k+n-1}) = x^{k+n},$$

so it is true for $m = k$. So by induction it is true for all $m \geq 0$.

If $m < 0$, and $y = x^{-1}$, then by the lemma $(x^m)(x^n) = (y^{-m})(y^{-n})$ which is equal to $y^{-(m+n)} = x^{m+n}$ by applying what we've already proved with y in place of x. □

We've already proved the formula $(xy)^{-1} = y^{-1}x^{-1}$. What about $(xy)^n$ for other values of n? In a non-abelian group, there is no simple formula. In particular:

WARNING: If x, y are elements of a non-abelian group, then in general $(xy)^n \neq x^n y^n$. The point is that (for $n > 0$, say)

$$(xy)^n = xyxy \dots xy$$

and unless the group is abelian we can not rearrange the terms to get

$$xx \dots xyy \dots y = x^n y^n.$$

4. An extended example: dihedral groups

As we study group theory, it will be useful to have a supply of examples of groups to think about. Of course, no single example will be ideal for everything, but some are more helpful than others. Some of the more "arithmetic" groups, such as $(\mathbb{Z}, +)$ and $(\mathbb{R} \setminus \{0\}, \times)$, have the adantage of being very familiar, but the disadvantage of being rather untypical because they're abelian. If you have a "standard example" that you like to think about, then it will be much less misleading if it's non-abelian. The symmetry groups of regular polygons are a good candidate, because they are non-abelian, but still fairly uncomplicated.

In this section we'll explicitly work through the details of this example.

First, some terminology.

Definition 4.1. The **order** $|G|$ of a group G is just the number of elements (possibly infinite) in G.

Note that the notation $|G|$ agrees with the standard notation used for the number of elements in a set.

Let X be a regular n-sided polygon, with vertices labelled anticlockwise $1, 2, \ldots, n$. Recall that by a **symmetry** of X we mean a permutation of the vertices that takes adjacent vertices to adjacent vertices.

For example, we can send vertex 1 to any other vertex by an appropriate rotation. If f is a symmetry sending vertex 1 to vertex i, then, since it preserves adjacency, it must send vertex 2 to one of the two vertices adjacent to vertex i, and once we know $f(1)$ and $f(2)$, then $f(3)$ is determined as the other vertex adjacent to $f(2)$, and so on around the polygon for $f(4), \ldots, f(n)$.

So the total number of symmetries (i.e., the **order** of the symmetry group) is $2n$ (since there are n choices for $f(1)$ and for each of these there are two choices for $f(2)$). This explains the following choice of notation.

Definition 4.2. The **dihedral group** D_{2n} of order $2n$ is the group of symmetries of a regular n-sided polygon.

Remark 4.1. Some books use the symbol D_n where we use D_{2n} (i.e., they label the group with the size of the polyon rather than the size of the group), although at least the D is fairly standard.

Let's fix some notation for two particular symmetries.

Definition 4.3. $a \in D_{2n}$ is a rotation anticlockwise through an angle of $2\pi/n$. $b \in D_{2n}$ is a reflection in the line through vertex 1 and the centre of the polygon.

So

$$a(1) = 2, a(2) = 3, \ldots, a(n-1) = n, a(n) = 1,$$

and

$$\dots b(n-1) = 3, b(n) = 2, b(1) = 1, b(2) = n, b(3) = n-1, \dots.$$

Now consider the symmetries a^i and $a^i b$ for $0 \leq i < n$. These both send vertex 1 to vertex $1+i$, but a^i sends vertices $2, 3, \dots, n$ to the vertices following anticlockwise around the polygon, whereas $a^i b$ sends them to the vertices following clockwise around the polygon. So all of these symmetries are different, and *every* symmetry is of this form, and so every element of D_{2n} can be written in terms of a and b.

Proposition 4.1. $D_{2n} = \{e, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$.

We'll use this as our standard form for elements, but other expressions, such as a^{-1} and ba, are in the group, so must be among those we've already listed.

There are three basic rules that let us easily do calculations.

Proposition 4.2. $a^n = e$.

This is clearly true, as it just says that if we repeat a rotation through an angle of $2\pi/n$ n times, then this is the same as the identity.

Note that this means that $a(a^{n-1}) = e$ and so by uniqueness of inverses

$$a^{-1} = a^{n-1},$$

which allows us to write any power (positive or negative) of a as one of $e, a, \dots, a^{n-1}$.

Proposition 4.3. $b^2 = e$.

This is clearly true, as repeating a reflection twice gives the identity.

This implies, by uniqueness of inverses again, that $b^{-1} = b$, and so any power of b is one of e or b.

What about ba? Well, $a(1) = 2$ and $b(2) = n$, so $ba(1) = n$ and the other vertices follow clockwise. This is the same as $a^{n-1}b$, or $a^{-1}b$.

Proposition 4.4. $ba = a^{n-1}b = a^{-1}b$.

We'll see that these three rules allow us to simplify any expression.

For example,

$$ba^{-1} = ba^{n-1} = baa^{n-2} = a^{-1}ba^{n-2} = a^{-1}baa^{n-3} = a^{-1}a^{-1}ba^{n-3} = \dots = a^{-n+1}b = ab,$$

and so "swap" a b with an a or a^{-1}, changing the a into a^{-1} or the a^{-1} into a.

So we get the following rules for multiplying expressions in standard form.

Theorem 4.5. *For* $0 \leq i, j < n$,

(1) $$a^i a^j = \begin{cases} a^{i+j} & \text{if } i+j < n \\ a^{i+j-n} & \text{if } i+j \geq n \end{cases}$$

$$(2)\ a^i(a^jb) = \begin{cases} a^{i+j}b & \text{if } i+j < n \\ a^{i+j-n}b & \text{if } i+j \geq n \end{cases}$$

$$(3)\ (a^ib)a^j = \begin{cases} a^{i-j}b & \text{if } i-j \geq 0 \\ a^{i-j+n}b & \text{if } i-j < 0 \end{cases}$$

$$(4)\ (a^ib)(a^jb) = \begin{cases} a^{i-j} & \text{if } i-j \geq 0 \\ a^{i-j+n} & \text{if } i-j < 0 \end{cases}$$

You are encouraged to practice some calculations with the dihedral group, especially with $n = 3$ and $n = 4$, as we'll frequently be using these as examples.

Remark 4.2. When $n = 3$, all vertices of a regular n-sided polygon (i.e., an equilateral triangle) are adjacent to one another, so D_6 contains **all** permutations of $\{1, 2, 3\}$. But this doesn't apply for larger n.

5. SUBGROUPS

Definition 5.1. A **subgroup** of a group G is a subset H of G that is itself a group with the same operation as G.

It is important that the group operation is the same. For example $\mathbb{R} \setminus \{0\}$ is a subset of $\mathbb{R}$, but we do not regard $(\mathbb{R} \setminus \{0\}, \times)$ as a subgroup of $(\mathbb{R}, +)$ since the group operations are different.

Example 5.1. For any group G, the **trivial subgroup** $\{e\}$ and G itself are subgroups of G.

We call a subgroup not equal to $\{e\}$ a **non-trivial** subgroup, and a subgroup not equal to G a **proper** subgroup of G.

Example 5.2. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

Example 5.3. The group $2\mathbb{Z}$ of even integers under addition is a subgroup of $(\mathbb{Z}, +)$.

Example 5.4. If n is a positive integer, then the group $n\mathbb{Z}$ of integers diisible by n, under addition, is a subgroup of $(\mathbb{Z}, +)$.

Example 5.5. The group of rotations of a regular n-sided polygon is a subgroup of the dihedral group D_{2n}.

Here's a simple description of what needs to be checked for a subset to be a subgroup.

Theorem 5.1. *Let G be a multiplicatively written group and let $H \subseteq G$ be a subset of G, Then H is a subgroup of G if and only if the following conditions are satisfied.*

- *(Closure) If $x, y \in H$ then $xy \in H$.*
- *(Identity) $e \in H$.*
- *(Inverses) If $x \in H$ then $x^{-1} \in H$.*

Proof. We **don't** need to check associativity, since $x(yz) = (xy)z$ is true for all elements of G, so is certainly true for all elements of H. So the conditions imply H is a group with the same operation as G.

If H is a group, then (Closure) must hold. By uniqueness of identity and inverses, the identity of H must be the same as that of G, and the inverse of $x \in H$ is the same in H as in G, so (Identity) and (Inverses) must hold. □

Proposition 5.2. *If H, K are two subgroups of a group G, then $H \cap K$ is also a subgroup of G.*

Proof. We check the three properties in the Theorem.

If $x, y \in H \cap K$ then $xy \in H$ by closure of H, and $xy \in K$ by closure of K, and so $xy \in H \cap K$.

$e \in H$ and $e \in K$, so $e \in H \cap K$.

If $x \in H \cap K$, then $x^{-1} \in H$ since H has inverses, and $x^{-1} \in K$ since K has inverses. So $x^{-1} \in H \cap K$. $\square$

6. ORDERS OF ELEMENTS

Definition 6.1. Let x be an element of a multiplicatively-written group G. Then:

- If $x^n = e$ for some positive integer n, then the least such positive integer n is called the **order** of x, and denoted by $\mathrm{ord}(x)$ (or $\mathrm{ord}_G(x)$ if it may be unclear what group G we're referring to).
- If there is no positive integer n such that $x^n = e$, then we say that x has **infinite order** and write $\mathrm{ord}(x) = \infty$ (or $\mathrm{ord}_G(x) = \infty$).

Remark 6.1. If you are asked to prove that $\mathrm{ord}(x) = n$, then as well as proving that $x^n = e$, remember that you also have to prove that n is the least positive integer for which this is true: in other words, prove that if $0 < m < n$ then $x^m \neq e$.

Remark 6.2. You may have noticed that the same word "order" is also used for the size of a group. Although the two meanings are different, we'll see in the next section that there is a very close relationship between them.

Example 6.1. In any group G with identity element e, $\mathrm{ord}(e) = 1$ and $x = e$ is the only element with $\mathrm{ord}(x) = 1$.

Example 6.2. In the dihedral group D_{2n}, with the notation of Section 4, $\mathrm{ord}(a) = n$ and $\mathrm{ord}(b) = 2$.

Example 6.3. In the group $(\mathbb{R} \setminus \{0\}, \times)$ of non-zero real numbers under multiplication, $\mathrm{ord}(1) = 1$, $\mathrm{ord}(-1) = 2$ (since $(-1)^2 = 1$ but $(-1)^1 \neq 1$), and for any other x $\mathrm{ord}(x) = \infty$ (since either $|x| < 0$, in which case $|x^n| < 0$ for all integers $n > 0$ and so $x^n \neq 1$, or $|x| > 0$, in which case $|x^n| > 0$ for all integers $n > 0$ and so $x^n \neq 1$.

Example 6.4. In the group $(\mathbb{C} \setminus \{0\}, \times)$ of non-zero complex numbers under multiplication, $\mathrm{ord}(i) = \mathrm{ord}(-i) = 4$.

Example 6.5. In the group $(\mathbb{Z}, +)$, $\mathrm{ord}(0) = 1$, but $\mathrm{ord}(s) = \infty$ for any other $s \in \mathbb{Z}$. Note that when the group operation is addition and the identity element is 0, as here, for an element s with finite order n we would require $s + s + \cdots + s$ (n times) to be 0.

We'll now see what we can say about the powers of an element of a group if we know its order, starting with elements of infinite order.

Proposition 6.1. *Let x be an element of a group G with $\mathrm{ord}(x) = \infty$. Then the powers x^i of x are all distinct: i.e., $x^i \neq x^j$ if $i \neq j$ are integers.*

Proof. Suppose $x^i = x^j$. Without loss of generality we'll assume $i \geq j$. Then for $n = i - j \geq 0$,

$$x^n = x^{i-j} = x^i(x^j)^{-1} = (x^i)(x^i)^{-1} = e,$$

but since $\mathrm{ord}(x) = \infty$ there is no positive integer n with $x^n = e$, so we must have $n = 0$ and so $i = j$. □

Corollary 6.2. *If x is an element of a finite group G, then $\mathrm{ord}(x) < \infty$.*

Proof. If $\mathrm{ord}(x) = \infty$ then the previous Proposition tells us that the elements x^i (for $i \in \mathbb{Z}$) are all different, and so G must have infinitely many elements. □

In fact, we'll see later that the order $|G|$ of a finite group severely restricts the possible (finite) orders of its elements.

Next for elements of finite order.

Proposition 6.3. *Let x be an element of a group G with $\mathrm{ord}(x) = n < \infty$.*

(1) *For an integer i, $x^i = e$ if and only if i is divisible by n.*
(2) *For integers i, j, $x^i = x^j$ if and only if $i - j$ is divisible by n [i.e., in terms of modular arithmetic, if and only if $i \equiv j \pmod{n}$].*
(3) $x^{-1} = x^{n-1}$.
(4) *The distinct powers of x are $e, x, x^2, \ldots, x^{n-1}$.*

Proof. (1) Firstly, if i is divisible by n, so that $i = nk$ for some integer k, then

$$x^i = x^{nk} = (x^n)^k = e^k = e,$$

since $x^n = e$.

Conversely, suppose that $x^i = e$. We can write $i = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. (I.e., by the "division algorithm" we can write i as a multiple of n plus a remainder r.) Then

$$e = x^i = x^{nq+r} = (x^n)^q x^r = e^q x^r = x^r.$$

But n is the least positive integer with $x^n = e$ and $x^r = e$ with $0 \leq r < n$, so r can't be positive, and we must have $r = 0$. So i is divisible by n.

(2) $x^i = x^j$ if and only if $x^{i-j} = x^i(x^j)^{-1} = e$, which by (1) is the case if and only if $i - j$ is divisible by n.
(3) Take $i = n - 1$, $j = -1$. Then $i - j = n$ is divisible by n, and so $x^{n-1} = x^{-1}$ by (2).
(4) For any integer i, write $i = nq + r$ for q, r integers with $0 \leq r < n$. Then $i - r$ is divisible by n, and so $x^i = x^r$ by (2). So every power of x is equal to one of $e = x^0, x = x^1, x^2, \ldots, x^{n-1}$. Conversely, If $i, j \in \{0, 1, \ldots, n-1\}$ and $i - j$ is divisible by n, then $i = j$, and so by (2) the elements $e, x, \ldots, x^{n-1}$ are all different.

□

If we know the order of an element of a group, then we can work out the order of any power of that element.

Proposition 6.4. *Let x be an element of a group G, and i an integer.*

(1) *If $\mathrm{ord}(x) = \infty$ and $i \neq 0$, then $\mathrm{ord}(x^i) = \infty$. (If $i = 0$, then $x^i = e$, and so $\mathrm{ord}(x^i = 1)$.*

(2) *If $\mathrm{ord}(x) = n < \infty$, then*

$$\mathrm{ord}(x^i) = \frac{n}{\mathrm{hcf}(n, i)},$$

(where $\mathrm{hcf}(n, i)$ denotes the highest common factor, or greatest common divisor, of n and i).

Proof. (1) Suppose $i > 0$. If $\mathrm{ord}(x^i) = m < \infty$, then $x^{im} = (x^i)^m = e$ with im a positive integer, contradicting $\mathrm{ord}(x) = \infty$. Similarly, if $i < 0$ then $x^{-im} = e$ with $-im$ a positive integer, again giving a contradiction. So in either case $\mathrm{ord}(x^i) = \infty$.

(2) Since $\mathrm{hcf}(n, i)$ divides i, n divides $\frac{ni}{\mathrm{hcf}(n,i)}$, and so

$$(x^i)^{\frac{n}{\mathrm{hcf}(n,i)}} = x^{\frac{ni}{\mathrm{hcf}(n,i)}} = e.$$

If $0 < m$ and $(x^i)^m = x^{im} = e$, then n divides im, so $\frac{n}{\mathrm{hcf}(n,i)}$ divides m, and in particular $\frac{n}{\mathrm{hcf}(n,i)} < m$. So $\frac{n}{\mathrm{hcf}(n,i)}$ is the smallest positive exponent d such that $(x^i)^d = e$, and is therefore the order of x^i.

□

Example 6.6. In the dihedral group D_{12}, $\mathrm{ord}(a) = 6$. So the Proposition gives $\mathrm{ord}(a^4) = 3$, since $\mathrm{hcf}(6, 4) = 2$.

Example 6.7. Taking $i = -1$, the Proposition gives $\mathrm{ord}(x^{-1}) = \mathrm{ord}(x)$, since $\mathrm{hcf}(n, -1) = 1$ for any n. [But this case is very easy to check directly, since $(x^{-1})^d = (x^d)^{-1}$ and so $x^d = e$ if and only if $(x^{-1})^d = e$.]

7. Cyclic groups and cyclic subgroups

Given a (multiplicatively-written) group G and an element $x \in G$, we'll define $\langle x \rangle$ to be the subset $\{x^i : i \in \mathbb{Z}\}$ of G consisting of all powers of x. It is easy to check that:

Proposition 7.1. *The set $\langle x \rangle$ is a subgroup of G.*

Proof. We need to check the conditions of Theorem 5.1.
If x^i, x^j are powers of x, then $x^i x^j = x^{i+j}$ is a power of x, so $\langle x \rangle$ is closed.
$e = x^0$ is a power of x, so $e \in \langle x \rangle$.
If $x^i \in \langle x \rangle$, then $(x^i)^{-1} = x^{-i} \in \langle x \rangle$, so $\langle x \rangle$ is closed under taking inverses. □

Definition 7.1. If $x \in G$, then $\langle x \rangle$ is called the **cyclic subgroup** of G **generated by** x.

The following explicit description of $\langle x \rangle$ follows immediately from Propositions 6.1 and 6.3.

Proposition 7.2. *If $\operatorname{ord}(x) = \infty$ then $\langle x \rangle$ is infinite with $x^i \neq x^j$ unless $i = j$.*
If $\operatorname{ord}(x) = n$ then $\langle x \rangle = \{e, x, \dots, x^{n-1}\}$ is finite, with n distinct elements.

This justifies using the word "order" in two different ways. The order (as an element) of x is the same as the order (as a group) of $\langle x \rangle$.

Example 7.1. If $G = D_{2n}$ is the dihedral group of order $2n$, then $\langle a \rangle$ is the group $\{e, a, \dots a^n\}$ of rotations, and $\langle b \rangle = \{e, b\}$.

Example 7.2. Let $G = (\mathbb{R} \setminus \{0\}, \times)$. Then $\langle -1 \rangle = \{1, -1\}$ and $\langle 2 \rangle = \{\dots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, \dots\}$ consists of all powers of 2 (and of $\frac{1}{2}$, since we include negative powers of 2.

Example 7.3. Let $G = (\mathbb{C} \setminus \{0\})$. Then $\langle i \rangle = \{1, i, -1, -i\}$.

Example 7.4. Let $G = (\mathbb{R}, +)$. Since the operation is now addition, $\langle x \rangle$ consists of all *multiples* of x. So, for example, $\langle 1 \rangle = \mathbb{Z}$ and $\langle 3 \rangle = 3\mathbb{Z} = \{3n : n \in \mathbb{Z}\}$.

Definition 7.2. A group G is called **cyclic** if $G = \langle x \rangle$ for some $x \in G$. Such an element x is called a **generator** of G.

Example 7.5. $(\mathbb{Z}, +)$ is cyclic, since $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, and 1 and -1 are generators.

This example shows that there may be more than one possible choice of generator. However, not every element is a generator, since, for example, $\langle 0 \rangle = \{0\}$ and $\langle 2 \rangle$ consists of only the even integers.

Example 7.6. Let H be the cyclic subgroup of D_{12} generated by a. Then a and a^{-1} are generators of H, but a^2 is not, since $\langle a^2 \rangle = \{e, a^2, a^4\}$ contains only the even powers of a.

Example 7.7. Let H be the cyclic subgroup of D_{14} generated by a. Then a^2 is a generator of H, since

$$\langle a \rangle = \{e, a^2, a^4, a^6, a^8 = a, a^{10} = a^3, a^{12} = a^5\}$$

contains all the powers of a. In fact, all elements of H except e are generators.

Proposition 7.3. *Every cyclic group is abelian.*

Proof. Suppose $G = \langle x \rangle$ is cyclic with a generator x. Then if $g, h \in G$, $g = x^i$ and $h = x^j$ for some integers i and j. So

$$gh = x^i x^j = x^{i+j} = x^j x^i = hg,$$

and so G is abelian. □

Of course, this means that not every group is cyclic, since no non-abelian group is. But there are also abelian groups, even finite ones, that are not cyclic.

Proposition 7.4. *Let G be a finite group with $|G| = n$. Then G is cyclic if and only if it has an element of order n. An element $x \in G$ is a generator if and only if* $\operatorname{ord}(x) = n$.

Proof. Suppose $x \in G$. Then $|\langle x \rangle| = \operatorname{ord}(x)$, and since $\langle x \rangle \leq G$, $\langle x \rangle = G$ if and only if $\operatorname{ord}(x) = |\langle x \rangle| = |G| = n$. □

Example 7.8. Let $G = D_8$ and let $H = \{e, a^2, b, a^2b\}$. Then H is an abelian subgroup of G (check this), but it is not cyclic, since $|H| = 4$ but $\operatorname{ord}(a^2) = \operatorname{ord}(b) = \operatorname{ord}(a^2b) = 2$ and $\operatorname{ord}(e) = 1$, so H has no element of order 4.

Notice that cyclic groups are particularly simple to understand if we know a generator, as the group operation is just addition of exponents: in a cyclic group $G = \langle x \rangle$, $x^i x^j = x^{i+j}$, so the group operation in an infinite cyclic group is "just like" addition of integers, and the group operation in a finite cyclic group of order n is "just like" addition of integers $\pmod n$. (We'll make "just like" more precise later.)

Theorem 7.5. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle x \rangle$ be a cyclic group with generator x, and let $H \leq G$ be a subgroup.

If $H = \{e\}$ is the trivial subgroup, then $H = \langle e \rangle$ is cyclic. Otherwise, $x^i \in H$ for some $i \neq 0$, and since also $x^{-i} \in H$ since H is closed under taking inverses, we can assume $i > 0$.

Let m be the smallest positive integer such that $x^m \in H$. We shall show that $H = \langle x^m \rangle$, and so H is cyclic.

Certainly $\langle x^m \rangle \subseteq H$, since every power of x^m is in H. Suppose $x^k \in H$ and write $k = mq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Then

$$x^r = x^{k-mq} = x^k (x^m)^q \in H,$$

since $x^k \in H$ and $x^m \in H$. But $0 \leq r < m$, and m is the smallest positive integer with $x^m \in H$, so $r = 0$ or we have a contradiction. So $x^k = (x^m)^q \in \langle x^m \rangle$. Since x^k was an arbitrary element of H, $H \subseteq \langle x^m \rangle$. $\square$

8. Groups from modular arithmetic

Let n be a positive integer. Recall that we say that integers a, b are "congruent $(\mathrm{mod}\ n)$" (and write $a \equiv b \pmod{n}$) if n divides $a-b$. Then there are n congruence classes $[0], [1], \ldots, [n-1]$ such that every integer is in exactly one class, depending on its remainder when we divide by n.

Recall also that there are well-defined operations of addition and multiplication $(\mathrm{mod}\ n)$, where

$$[a] + [b] = [a + b] \text{ and } [a][b] = [ab]$$

don't depend on which choice of elements a and b we make from the congruence class.

We'll write $\mathbb{Z}/n\mathbb{Z}$ for the set of congruence classes, and will often write a instead of $[a]$ when it's clear that we're considering it as an element of $\mathbb{Z}/n\mathbb{Z}$.

Example 8.1. The distinct elements of $\mathbb{Z}/7\mathbb{Z}$ are $0, 1, 2, 3, 4, 5, 6$. In $\mathbb{Z}/7\mathbb{Z}$, $7 = 0$ $-3 = 4$, $-8 = 6$, etc.

Theorem 8.1. $(\mathbb{Z}/n\mathbb{Z}, +)$ *is an abelian group.*

Proof. $\mathbb{Z}/n\mathbb{Z}$ is closed under addition. Addition $(\mathrm{mod}\ n)$ is associative, since

$$([a] + [b]) + [c] = [a + b + c] = [a] + ([b] + [c]).$$

The identity element is $[0]$ since

$$[a] + [0] = [a] = [0] + [a]$$

for any $a \in \mathbb{Z}$. The inverse of $[a]$ is $[-a]$, since

$$[a] + [-a] = [0] = [-a] + [a].$$

So $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group. It is abelian since $[a] + [b] = [a + b] = [b + a]$ for all a and b. □

In fact, it is a cyclic group, since the following is clear.

Proposition 8.2. $(\mathbb{Z}/n\mathbb{Z}, +) = \langle 1 \rangle$.

However, $(\mathbb{Z}/n\mathbb{Z}, \times)$ is not a group, since although it is associative and has an identity element $[1]$, not every element has an inverse. For example, $[0]$ never has an inverse, and in $\mathbb{Z}/4\mathbb{Z}$, $[2]$ does not have a multiplicative inverse.

Proposition 8.3. *In* $\mathbb{Z}/n\mathbb{Z}$, $[a]$ *has a multiplicative inverse if and only if* $\mathrm{hcf}(a, n) = 1$.

Proof. If $\mathrm{hcf}(a, n) = 1$ then recall that Euclid's algorithm implies that $as + nt = 1$ for some $s, t \in \mathbb{Z}$. So

$$as \equiv 1 - nt \equiv 1 \pmod{n},$$

so $[a][s] = [1]$ in $\mathbb{Z}/n\mathbb{Z}$, and so $[s]$ is a multiplicative inverse of $[a]$.

Conversely, if $\text{hcf}(a, n) = h > 1$, and if $as \equiv 1 \pmod{n}$, then $1 = as + nq$ for some $q \in \mathbb{Z}$. But h divides both a and n, so it divides $as + nq$. But no integer $h > 1$ divides 1. So there is no s such that $[s]$ is a multiplicative inverse of a. □

Note that the first part of the proof gives a method for finding the inverse of an element (when it has one) using Euclid's algorithm.

Definition 8.1. U_n is the subset $\{[a] : a \in \mathbb{Z} \text{ and } \text{hcf}(a, n) = 1\}$ of $\mathbb{Z}/n$.

Remark 8.1. If $\text{hcf}(a, n) = 1$ then $\text{hcf}(a + nt, n) = 1$ for any $t \in \mathbb{Z}$ and so it makes no difference which element of $[a]$ we use to check the condition for $[a] \in U_n$. Since every congruence class $[a]$ contains an element a with $0 \leq a < n$, we'll usually use these elements.

Example 8.2. If p is a prime, then $U_p = \{[1], [2], \ldots, [p-1]\}$ has order $p - 1$.

Example 8.3. $U_4 = \{[1], [3]\}$, $U_6 = \{[1], [5]\}$ both have order 2. $U_8 = \{[1], [3], [5], [7]\}$ and $U_{10} = \{[1], [3], [7], [9]\}$ have order 4.

Theorem 8.4. $(U_n, \times)$ *is an abelian group.*

Proof. Suppose $[a], [b] \in U_n$, so $\text{hcf}(a, n) = 1 = \text{hcf}(b, n)$. Then $\text{hcf}(ab, n) = 1$ and so $[ab] \in U_n$ and U_n is closed under multiplication.

Since

$$([a][b])[c] = [abc] = [a]([b][c])$$

multiplication on U_n is associative.

$[1]$ is an identity element, since $[1][a] = [a] = [a][1]$ for any a.

If $[a] \in U_n$, so $\text{hcf}(a, n) = 1$, then $as + nt = 1$ for integers s, t, and $\text{hcf}(s, t) = 1$. So $[s] \in U_n$ is an inverse of $[a]$.

So U_n is a group under multiplication. It is abelian since $[a][b] = [ab] = [b][a]$ for all $a, b \in \mathbb{Z}$. □

Unlike $(\mathbb{Z}/n\mathbb{Z}, +)$, $(U_n, \times)$ is not always cyclic (although it sometimes is).

Example 8.4. U_{10} is cyclic, with generator $[7]$: $[7]^0 = [1]$, $[7]^1 = [7]$, $[7]^2 = [49] = [9]$, $[7]^3 = [7][9] = [63] = [3]$, so

$$\langle [7] \rangle = \{[1], [3], [7], [9]\rangle = U_{10}.$$

Example 8.5. U_8 is not cyclic. $[3]^2 = [9] = [1]$, $[5]^2 = [25] = [1]$ and $[7]^2 = [49] = [1]$, so every element has order 2 apart from $[1]$, which has order 1. In particular there are no elements of order $|U_8| = 4$, so the group is not cyclic.

Remark 8.2. In fact, U_n is cyclic if and only if $n = 2$, $n = 4$ or $n = p^r$ or $n = 2p^r$ for p an odd prime and $r \geq 1$, but this is beyond the scope of this unit.

9. ISOMORPHIC GROUPS

Suppose $G = \langle x \rangle = \{e, x, x^2\}$ and $H = \langle y \rangle = \{e, y, y^2\}$ are two cyclic groups of order 3. Strictly speaking they are different groups, since (for example) x is an element of G but not of H. But clearly they are "really the same" in some sense: the only differences are the names of the elements, and the "abstract structure" of the two groups is the same. To make this idea, of two groups being abstractly the same, precise, we introduce the idea of an isomorphism of groups.

Definition 9.1. Let $(G, *)$ and $(H, \bullet)$ be groups. An **isomorphism** from G to H is a bijective function $\varphi : G \to H$ such that

$$\varphi(x * y) = \varphi(x) \bullet \varphi(y)$$

for all elements $x, y \in G$.

Remark 9.1. We used different symbols for the two group operations to point out that the isomorphism links the two different operations. As ever, we'll usually write the groups multiplicatively, in which case the defining property of an isomorphism becomes

$$\varphi(xy) = \varphi(x)\varphi(y),$$

but it should be stressed that this involves two different kinds of "multiplication": on the left hand side of the equation we are multiplying in G, but on the right hand side in H.

Example 9.1. Let $G = \langle x \rangle$ and $H = \langle y \rangle$ be two cyclic groups of the same order. Then $\varphi : G \to H$ defined by $\varphi(x^i) = y^i$ for every $i \in \mathbb{Z}$ is an isomorphism, since it is a bijection and

$$\varphi(x^{i+j}) = y^{i+j} = y^i y^j = \varphi(x^i)\varphi(x^j)$$

for all i, j.

Remark 9.2. Since φ is a bijection, it pairs off elements of G with elements of H, and then the defining property of an isomorphism says that we can use φ and its inverse φ^{-1} as a dictionary to translate between elements of G and elements of H without messing up the group operation. If we take the multiplication (Cayley) table of G and apply φ to all the entries, we get the multiplication table of H: the groups G and H are "really the same" apart from the names of the individual elements.

Next we'll prove some of the easy consequences of the definition.

Proposition 9.1. *Let $\varphi : G \to H$ be an isomorphism between (multiplicatively-written) groups. Then $\varphi^{-1} : H \to G$ is also an isomorphism.*

Proof. Since φ is a bijection, it does have an inverse function φ^{-1} that is also a bijection.

Let $u, v \in H$. Since φ is a bijection, there are unique elements $x, y \in G$ with $u = \varphi(x)$ and $v = \varphi(y)$. Then

$$\varphi^{-1}(uv) = \varphi^{-1}(\varphi(x)\varphi(y)) = \varphi^{-1}(\varphi(xy)) = xy = \varphi^{-1}(u)\varphi^{-1}(v),$$

and so φ^{-1} is an isomorphism. □

Because of this Proposition, the following definition makes sense, since it tells us that there is an isomorphism from G to H if an only if there is one from H to G.

Definition 9.2. Two groups G and H are said to be **isomorphic**, or we say G is **isomorphic to** H, if there is an isomorphism $\varphi : G \to H$, and then we write $G \cong H$, or $\varphi : G \cong H$ if we want to specify an isomorphism.

Proposition 9.2. *Let G, H, K be three groups. If G is isomorphic to H and H is isomorphic to K, then G is isomorphic to K.*

Proof. Let $\varphi : G \to H$ and $\theta : H \to K$ be isomorphisms. Then the composition $\theta\varphi : G \to K$ is a bijection and if $x, y \in G$ then

$$\theta(\varphi(xy)) = \theta(\varphi(x)\varphi(y)) = \theta(\varphi(x))\,\theta(\varphi(y)),$$

and so $\theta\varphi$ is an isomorphism. □

Remark 9.3. This says that the relation "being isomorphic" is transitive. It is also symmetric by Prop. 9.1, and is clearly relexive (a group G is isomorphic to itself since the identity function $\mathrm{id}_G : G \to G$ is an isomorphism). So the relation is an equivalence relation on the class of all groups.

Proposition 9.3. *Let $\varphi : G \to H$ be an isomorphism between (multiplicatively-written) groups, let e_G and e_H be the identity elements of G and H respectively, and let $x \in G$. Then*

(1) $\varphi(e_G) = e_H$,
(2) $\varphi(x^{-1}) = \varphi(x)^{-1}$.
(3) $\varphi(x^i) = \varphi(x)^i$ *for every* $i \in \mathbb{Z}$.
(4) $\mathrm{ord}_G(x) = \mathrm{ord}_H(\varphi(x))$.

Proof.
(1) $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$, and so by uniqueness of the identity, $\varphi(e_G)$ is the identity element of H.
(2) $e_H = \varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, and so by uniqueness of inverses $\varphi(x^{-1})$ is the inverse of $\varphi(x)$.
(3) The statement is true for $i = 1$, and follows by induction for positive i, since if $\varphi(x^i) = \varphi(x)^i$ then

$$\varphi(x^{i+1}) = \varphi(x^i x) = \varphi(x^i)\varphi(x) = \varphi(x)^i\varphi(x) = \varphi(x)^{i+1}.$$

The statement is true for $i = 0$ by (1), and follows for $i < 0$ by (2), since then

$$\varphi(x^i) = \varphi\left((x^{-i})^{-1}\right) = \varphi(x^{-i})^{-1} = \left(\varphi(x)^{-i}\right)^{-1} = \varphi(x)^i.$$

(4) By (1) and (3), $x^i = e_G \Leftrightarrow \varphi(x)^i = e_H$, and so $\mathrm{ord}_G(x) = \mathrm{ord}_H(\varphi(x))$.

□

To prove that two groups are isomorphic usually requires finding an explicit isomorphism. Proving that two groups are **not** isomorphic is often easier, as if we can find an "abstract property" that distinguishes them, then this is enough, since isomorphic groups have the same "abstract properties". We'll make this precise, and prove it, with some typical properties, after which you should be able to see how to give similar proofs for other properties, just using an isomorphism to translate between properties of G and of H..

Proposition 9.4. *Let* G *and* H *be isomorphic groups. Then they have the same order (i.e., the same number of elements).*

Proof. This follows just from the fact that an isomorphism is a bijection $\varphi : G \to H$. □

Proposition 9.5. *Let* G *and* H *be isomorphic groups. If* H *is abelian then so is* G.

Proof. Suppose that $\varphi : G \to H$ is an isomorphism and that H is abelian. Let $x, y \in G$. Then

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi(y)\varphi(x) = \varphi(yx),$$

since $\varphi(x), \varphi(y) \in H$, which is abelian. Since φ is a bijection (and in particular injective) it follows that $xy = yx$. So G is abelian. □

Proposition 9.6. *Let* G *and* H *be isomorphic groups. If* H *is cyclic then so is* G.

Proof. Suppose $\varphi : G \to H$ is an isomorphism and $H = \langle y \rangle$ is cyclic. So every element of H is a power of y. So if $g \in G$ then $\varphi(g) = y^i$ for some $i \in \mathbb{Z}$, and so $g = \varphi^{-1}(y)^i$. So if $x = \varphi^{-1}(y)$ then every element of G is a power of x, and so $G = \langle x \rangle$. □

Proposition 9.7. *Let* G *and* H *be isomorphic groups and* n *a positive integer (or* $n = \infty$*). Then* G *and* H *have the same number of elements of order* n*.*

Proof. By Prop. 9.3, an isomorphism $\varphi : G \to H$ induces a bijection between the set of elements of G with order n and the set of elements of H with order n. □

The idea of isomorphism gives an important tool for understanding unfamiliar or difficult groups. If we can prove that such a group is isomorphic to a group that we understand well, then this is a huge step forward.

The following example of a group isomorphism was used for very practical purposes in the past.

Example 9.2. The logarithm function

$$\log_{10} : (\mathbb{R}_{>0}, \times) \to (\mathbb{R}, +)$$

is an isomorphism from the group of positive real numbers under multiplication to the group of real numbers under addition (of course we could use any base for the logarithms). It is a bijection since the function $y \mapsto 10^y$ is the inverse function, and the group isomorphism property is the familiar property of logarithms that

$$\log_{10}(ab) = \log_{10}(a) + \log_{10}(b).$$

Now, if you don't have a calculator, then addition is much easier to do by hand than multiplication, and people used to use "log tables" to make multiplication easier. If they wanted to multiply two numbers, they would look up the logarithms, add them and then look up the "antilogarithm".

In group theoretic language they were exploiting the fact that there is an isomorphism between the "difficult" group $(\mathbb{R}_{>0}, \times)$ and the "easy" group $(\mathbb{R}, +)$.

10. DIRECT PRODUCTS

In this section we'll study a simple way of combining two groups to build a new, larger, group. Recall that if X and Y are sets, then the **Cartesian product** $X \times Y$ is the set whose elements are **ordered pairs** (x, y) whose first coordinate x is an element of X, and whose second coordinate y is an element of Y. I.e.,

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

Definition 10.1. Let H and K be (multiplicatively-written) groups. The **direct product** $H \times K$ of H and K is the Cartesian product of the sets H and K, with the binary operation

$$(x, y)(x', y') = (xx', yy')$$

for $x, x' \in H$ and $y, y' \in K$.

Proposition 10.1. *The direct product $H \times K$ of groups is itself a group.*

Proof. Associativity of $H \times K$ follows from associativity of H and K, since if $x, x', x" \in H$ and $y, y', y" \in K$, then

$$\begin{aligned}((x, y)(x', y'))\,(x", y") &= (xx', yy')(x", y") \\ &= (xx'x", yy'y") \\ &= (x, y)(x'x", y'y") \\ &= (x, y)\,((x', y')(x", y")).\end{aligned}$$

If e_H and e_K are the identity elements of H and K, then (e_H, e_K) is the identity element of $H \times K$, since if $x \in H$ and $y \in K$, then

$$(e_H, e_K)(x, y) = (e_H x, e_K y) = (x, y) = (x e_H, y e_K) = (x, y)(e_H, e_K).$$

The inverse of $(x, y) \in H \times K$ is (x^{-1}, y^{-1}), since

$$(x, y)(x^{-1}, y^{-1}) = (xx^{-1}, yy^{-1}) = (e_H, e_K) = (x^{-1}x, y^{-1}y) = (x^{-1}, y^{-1})(x, y).$$

□

Notice that for all aspects of the group structure, we simply apply the corresponding idea in the first coordinate for H and in the second coordinate for K. This is generally how we understand $H \times K$, by considering the two coordinates separately, and if we understand H and K, then $H \times K$ is easy to understand. For example, it is easy to see that, for any $i \in \mathbb{Z}$ and any $(x, y) \in H \times K$,

$$(x, y)^i = (x^i, y^i),$$

so also taking powers in a direct product is just a matter of taking powers of the coordinates separately.

Here are some very easy consequences of the definition.

Proposition 10.2. *Let* H *and* K *be (multiplicatively-written) groups, and let* $G = H \times K$ *be the direct product.*

(1) G *is finite if and only if both* H *and* K *are finite, in which case* $|G| = |H||K|$.
(2) G *is abelian if and only if both* H *and* K *are abelian.*
(3) *If* G *is cyclic then both* H *and* K *are cyclic.*

Proof. (1) This is just a familiar property of Cartesian products of sets.

(2) Suppose H and K are abelian, and let $(x, y), (x', y') \in G$. Then

$$(x, y)(x', y') = (xx', yy') = (x'x, y'y) = (x', y')(x, y),$$

and so G is abelian.

Suppose G is abelian, and $x, x' \in H$, Then

$$(xx', e_K) = (x, e_K)(x', e_K) = (x', e_K)(x, e_K) = (x'x, e_K),$$

and considering the first coordinates, $xx' = x'x$, and so H is abelian. Similarly K is abelian.

(3) Suppose G is cyclic, and (x, y) is a generator, so that every element of G is a power of (x, y). Let $x' \in H$. Then $(x', e_K) \in G$, so $(x', e_K) = (x, y)^i = (x^i, y^i)$ for some $i \in \mathbb{Z}$, and so $x' = x^i$. So every element of H is a power of x, so $H = \langle x \rangle$ is cyclic. Similarly K is cyclic.

□

Remark 10.1. The converse of (3) is not true in general: the direct product of cyclic groups may not be cyclic. For example, if H and K are both cyclic of order 2, then $(x, y)^2 = (e_H, e_K)$ for every $(x, y) \in H \times K$, so $H \times K$ has no element of order $|H \times K| = 4$, and so can't be cyclic.

Proposition 10.3. *Let* H *and* K *be (multiplicatively-written) groups, and* $x \in H$, $y \in K$ *elements with finite order. Then* $(x, y) \in H \times K$ *has finite order equal to the least common multiple*

$$\operatorname{lcm}\left(\operatorname{ord}_H(x), \operatorname{ord}_K(y)\right).$$

Proof. Let $i \in \mathbb{Z}$. Then $(x, y)^i = (e_H, e_K)$ if and only if $x^i = e_H$ and $y^i = e_K$, which is the case if and only if i is divisible by both $\operatorname{ord}_H(x)$ and by $\operatorname{ord}_K(y)$. The least positive such i is $\operatorname{lcm}\left(\operatorname{ord}_H(x), \operatorname{ord}_K(y)\right)$, and so this is tthe order of (x, y). □

We can now decide precisely when the direct product of cyclic groups is cyclic.

Theorem 10.4. *Let* H *and* K *be finite cyclic groups. Then* $H \times K$ *is cyclic if and only if* $\operatorname{hcf}(|H|, |K|) = 1$.

Proof. Let $(x, y) \in H \times K$. Then $\operatorname{ord}_H(x) \leq |H|$ and $\operatorname{ord}_K(y) \leq |K|$. So by Proposition 10.3,

$$\operatorname{ord}_{H \times K}(x, y) = \operatorname{lcm}\left(\operatorname{ord}_H(x), \operatorname{ord}_K(y)\right) \leq \operatorname{ord}_H(x) \operatorname{ord}_K(y) \leq |H||K|,$$

where the first inequality is an equality if and only if $\mathrm{ord}_H(x)$ and $\mathrm{ord}_K(y)$ are coprime, and the second inequality is an equality if and only if $H = \langle x \rangle$ and $K = \langle y \rangle$.

Since $|H \times K| = |H||K|$, $H \times K$ is cyclic if and only if it has an element of order $|H||K|$, which by the argument above is true if and only if $\mathrm{hcf}(\mathrm{ord}_H(x), \mathrm{ord}_K(y)) = 1$. □

Notation: If $n > 0$ is an integer, we'll use the notation C_n for a (multiplicatively-written) cyclic group of order n.

Since cyclic groups of the same order are isomorphic, the last theorem says that

$$C_m \times C_n \cong C_{mn}$$

if and only if $\mathrm{hcf}(m, n) = 1$.

Example 10.1. $C_2 \times C_2$ and $C_4 \times C_2$ are not cyclic.

Remark 10.2. $C_2 \times C_2$ is an abelian group of order 4 such that every element apart from the identity has order 2. It is easy to check that if $G = \{e, a, b, c\}$ is any group with these properties, then $ab = c = ba$, $ac = b = ca$ and $bc = a = cb$: i.e., the product of any two of the three non-identity elements is the other non-identity element. This means that there is only one possible multiplication table for such a group, and so any two groups with these properties are isomorphic.

Definition 10.2. A **Klein 4-group** is a group of order 4 such that every element except the identity has order 2.

Remark 10.3. This is named after the German mathematician Felix Klein. You need to be *really* famous to have something this trivial named after you! We'll see later that every group of order 4 is either cyclic or a Klein 4-group.

Example 10.2. We saw in Example 8.5 that the group U_8 is a Klein 4-group.

Example 10.3.
(1) $C_2 \times C_3 \cong C_6$
(2) $C_2 \times C_9 \cong C_{18}$
(3) $C_{90} \cong C_2 \times C_{45} \cong C_2 \times (C_9 \times C_5)$

We can clearly extend the definition of a direct product of two groups to three, four or more groups and make sense of things like $G \times H \times K$, which would be a group whose elements are the ordered triples (x, y, z) with $x \in G$, $y \in H$ and $z \in K$.

We can then write Example 10.3(3) as

$$C_{90} \cong C_2 \times C_9 \times C_5.$$

More generally, if $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, where $p_1, p_2, \dots, p_k$ are distinct primes, then

$$C_n \cong C_{p_1^{r_1}} \times C_{p_2^{r_2}} \times \cdots \times C_{p_k^{r_k}},$$

so that every finite cyclic group is isomorphic to a direct product of groups with order powers of primes.

We'll finish this section with some rather different examples of familiar groups that are isomorphic to direct products.

Proposition 10.5. $(\mathbb{R} \setminus \{0\}, \times) \cong (\mathbb{R}_{>0}, \times) \times (\{1, -1\}, \times)$.

Proof. Define a map

$$\varphi : \mathbb{R}_{>0} \times \{1, -1\} \to \mathbb{R} \setminus \{0\}$$

by $\varphi(x, \varepsilon) = \varepsilon x$. This is clearly a bijection, and

$$\varphi\left((x, \varepsilon)(x'\varepsilon')\right) = \varphi(xx', \varepsilon\varepsilon') = \varepsilon\varepsilon' xx' = (\varepsilon x)(\varepsilon' x') = \varphi(x, \varepsilon)\varphi(x', \varepsilon'),$$

so that φ is an isomorphism. □

Proposition 10.6. *Let* m, n *be positive integers with* $\mathrm{hcf}(m, n) = 1$. *Then*

$$U_{mn} \cong U_m \times U_n.$$

Proof. Define a map

$$\varphi : U_{mn} \to U_m \times U_n$$

by $\varphi([a]_{mn}) = ([a]_m, [a]_n)$ (where we use subscripts such as $[a]_m$ to indicate a congruence class $\pmod n$). This makes sense, since if $\mathrm{hcf}(a, mn) = 1$, then $\mathrm{hcf}(a, m) = 1$ and $\mathrm{hcf}(a, n) = 1$.

φ is injective, since if $a \equiv b \pmod m$ and $a \equiv b \pmod n$ then (since $\mathrm{hcf}(m, n) = 1$) $a \equiv b \pmod{mn}$.

The fact that φ is surjective is just the Chinese Remainder Theorem (which you'll have met in Foundations and Proof if you took that unit), which states that if $\mathrm{hcf}(m, n) = 1$ then for any $c, d \in \mathbb{Z}$ there is some $a \in \mathbb{Z}$ with $a \equiv b \pmod m$ and $a \equiv c \pmod n$. If $\mathrm{hcf}(b, m) = 1$ and $\mathrm{hcf}(c, n) = 1$, then $\mathrm{hcf}(a, mn) = 1$.

Since φ is bijective, and

$$\varphi([a]_{mn}[a']_{mn}) = ([aa']_m, [aa']_n) = ([a]_m, [a]_n)([a']_m, [a']_n) = \varphi([a]_{mn})\varphi([a']_{mn}),$$

φ is an isomorphism. □

Remark 10.4. The conclusion of Proposition 10.6 is not true if $\mathrm{hcf}(m, n) \neq 1$. For example, $|U_4| = 2$, but $|U_{16}| = 8$, so U_{16} can't be isomorphic to $U_4 \times U_4$.

11. LAGRANGE'S THEOREM

Let $G = D_{2n}$ be the dihedral group of order $2n$, and consider the orders of elements. Every reflection has order 2, which divides $|G|$. The rotation a has order n, which divides $|G|$. Every other rotation a^i has order $n/\operatorname{hcf}(n,i)$, which divides $|G|$. In this section we'll show that this is a general phenomenon for finite groups. In fact, we'll prove a more general fact about orders of subgroups (of course, this includes the case of the order of an element x, since $\operatorname{ord}(x)$ is equal to the order of the cyclic subgroup $\langle x\rangle$ generated by x).

The theorem in question is named after the eighteenth century Italian mathematician Lagrange, who proved a special case of the theorem before the days of abstract group theory.

Theorem 11.1 (Lagrange's Theorem)**.** *Let G be a finite group, and $H \leq G$ a subgroup. Then $|H|$ divides $|G|$.*

The idea of the proof is to split up G into subsets, each with the same number of elements as H, so that no two of these subsets overlap (i.e., every element of G is in exactly one of the subsets, so that $|G|$ is just the number of these subsets times $|H|$.

Definition 11.1. Let $H \leq G$ and $x \in G$. The **left coset** xH is the subset

$$xH = \{xh \in G : h \in H\}.$$

Remark 11.1. This is a sub**set** of G, but not usually a sub**group** since the identity element e is only in xH if $e = xh$ for some $h \in H$, in which case $x = h^{-1}$ and so $x \in H$. So xH is only a subgroup if $x \in H$, in which case $xH = H$.

Remark 11.2. We could also define a **right coset** Hx in the obvious way. In general this may be different from xH, but it would make little difference to what follows if we used right cosets instead of left cosets.

Once we have the idea of looking at left cosets, the properties we need are easy to check.

First, for fixed G and H, all left cosets xH have the same number of elements.

Lemma 11.2. *Let $H \leq G$ and $x \in G$. Then there is a bijection $\alpha : H \to xH$, so that $|xH| = |H|$.*

Proof. Define α by $\alpha(h) = xh$. Then α is surjective, since by definition every element of xH is of the form $xh = \alpha(h)$ for some $h \in H$. But also α is injective, since if $h, h' \in H$ then

$$\alpha(h) = \alpha(h') \Rightarrow xh = xh' \Rightarrow h = h'.$$

□

Next we prove that if two left cosets intersect non-trivially, then they are equal.

Lemma 11.3. *Let* $H \leq G$ *and* $x, y \in G$. *Then* $xH \cap yH \neq \emptyset$ *if and only if* $xH = yH$.

Proof. Suppose $xH \cap yH \neq \emptyset$, and choose $g \in xH \cap yH$. Then $g = xa = yb$ for some $a, b \in H$, so that $x = yba^{-1}$. If $h \in H$ then $xh = y(ba^{-1}h) \in yH$ since $ba^{-1}h \in H$. So every element of xH is in yH. Similarly every element of yH is in xH, so that $xH = yH$. □

Now we can easily put everything together to prove Lagrange's Theorem.

Proof of Theorem 11.1. Suppose that k is the number of distinct left cosets xH. Every element $g \in G$ is in one of the left cosets, since $g = ge \in gH$. By the two previous lemmas, every element of G is in exactly one of the k cosets, each of which contains $|H|$ elements. So the number of elements of G is $k|H|$. □

Example 11.1. Let $G = D_3$ be the dihedral group of order 6 and let $H = \langle a \rangle = \{e, a, a^2\}$ be the cyclic subgroup generated by a. If $x \in H$, then $xH = H$. If $x \notin H$, so $x = ba^i$ for some i, then $xH = \{ba^i, ba^{i+1}, ba^{i+2}\} = bH$. So there are two left cosets $\{e, a, a^2\}$ and $\{b, ba, ba^2\}$. [In this case the right cosets are the same as the left cosets.]

Example 11.2. Let $G = D_6$ again, but let $H = \langle b \rangle = \{e, b\}$ be the cyclic subgroup generated by b. Then

- $eH = \{e, b\} = bH$,
- $aH = \{a, ab\} = abH$,
- $a^2H = \{a^2, a^2b\} = a^2bH$,

so there are three left cosets. [In this case the right cosets are different, since for example $Ha = \{a, ba\} = \{a, a^2b\}$, which is not a left coset.]

Definition 11.2. Let $H \leq G$. Then the **index** $|G : H|$ is the number (possibly infinite if G is infinite) of left cosets xH in G.

Remark 11.3. So the proof of Lagrange's Theorem shows that

$$|G| = |H||G : H|$$

if G is finite.

Remark 11.4. Even if G is infinite, the index $|G : H|$ may be finite. For example, let $G = (\mathbb{Z}, +)$ and let $H = 2\mathbb{Z}$ be the subgroup of even integers. Then there are two left cosets: the set H of even integers, and the set of odd integers. So $|G : H| = 2$. Similarly $|\mathbb{Z} : n\mathbb{Z}| = n$ for any positive integer n, with the left cosets being the congruence classes $(\mathrm{mod}\ n)$.

12. Some consequences and applications of Lagrange's Theorem

As explained at the beginning of the last section, one immediate consequence of Lagrange's Theorem is to orders of elements.

Corollary 12.1 (Lagrange for orders of elements)**.** *Let* G *be a finite group with* $|G| = n$*. Then for any* $x \in G$*, the order of* x *divides* n*, and so* $x^n = e$*.*

Proof. By Lagrange's Theorem, the order of the cyclic subgroup $\langle x \rangle$ divides n. But the order of this subgroup is just $\text{ord}(x)$, so $\text{ord}(x)$ divides n, and so $x^n = e$. □

Applying this to some familiar groups, this has consequences that are interesting and useful outside group theory.

Theorem 12.2 (Fermat's Little Theorem)**.** *Let* p *be a prime and* a *an integer not divisible by* p*. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. We'll apply Corollary 12.1 to the group $G = U_p$. Since p is prime, $U_p = \{[1], [2], \ldots, [p-1]\}$ has order $p-1$, and if a is not divisible by p then $[a] \in U_p$. So by Corollary 12.1,

$$[a]^{p-1} = [1]$$

in U_p, or in other words

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

This simplifies calculating powers of integers modulo a prime:

Example 12.1. Suppose we want to calculate $7^{100} \pmod{31}$. The straightforward way to do this would involve multiplying by seven 99 times (although even without Fermat's Little Theorem a more intelligent approach would use many fewer multiplications). But by Fermat's Little Theorem with $p = 31$,

$$7^{30} \equiv 1 \pmod{31},$$

and so

$$7^{100} = (7^{30})^3 \times 7^{10} \equiv 1^3 \times 7^{10} \pmod{31}.$$

So without much calculation at all we reduce the problem to calculating a tenth power instead of a hundredth power. And then, to finish, $7^2 = 49 \equiv 18 \pmod{31}$, so $7^3 \equiv 7 \times 18 = 126 \equiv 2 \pmod{31}$ and

$$7^{10} = (7^3)^3 \times 7 \equiv 2^3 \times 7 = 56 \equiv 25 \pmod{31}.$$

There is a generalization to powers modulo m where m is not prime, but the statement is a bit more complicated, since U_m is not just $\{[1], [2], \ldots, [m-1]\}$. So first, let's inttroduce some standard notation for the order of this group.

Definition 12.1. Euler's phi function is the function φ from positive integers to positive integers with $\varphi(m)$ equal to the number of integers a such that $0 < a \leq m$ and $\text{hcf}(a, m) = 1$.

Remark 12.1. This is precisely the order of U_m, since $U_m = \{[a] : \text{hcf}(a, m) = 1\}$.

Example 12.2. If p is prime, then $\varphi(p) = p - 1$.

Theorem 12.3 (Fermat-Euler Theorem)**.** *Let* $m > 0$ *and* a *be integers with* $\text{hcf}(a, m) = 1$*. Then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Proof. Apply Theorem 12.1 to the group $G = U_m$. The condition $\text{hcf}(a, m) = 1$ means that $[a] \in U_m$, and $|U_m| = \varphi(m)$, so the theorem gives

$$[a]^{\varphi(m)} = [1]$$

in U_m, or in other words

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

□

Lagrange's Theorem gives most information about a group when the order of the group has relatively few factors, as then it puts more restrictions on possible orders of subgroups and elements.

Let's consider the extreme case, when the order of the group is a prime p, and so the only factors are 1 and p.

Theorem 12.4. *Let* p *be a prime and* G *a group with* $|G| = p$*. Then*

(1) G *is cyclic.*
(2) *Every element of* G *except the identity has order* p *and generates* G*.*
(3) *The only subgroups of* G *are the trivial subgroup* $\{e\}$ *and* G *itself.*

Proof. Let $x \in G$ with $x \neq e$. Then $\text{ord}(x)$ divides $|G| = p$ by Corollary 12.1, and $\text{ord}(x) \neq 1$ since $x \neq e$. So $\text{ord}(x) = p$. So the cyclic subgroup $\langle x \rangle$ generated by x has order p, and so must be the whole of G. This proves (1) and (2).

Let $H \leq G$. Then by Theorem 11.1 $|H|$ divides $|G| = p$, and so $|H| = 1$, in which case H is the trivial subgroup $\{e\}$, or $|H| = p$, in which case $H = G$. □

Remark 12.2. In particular this shows that if p is prime then all groups of order p are isomorphic.

Corollary 12.5. *If* p *is prime and* P *and* Q *are two subgroups of a group* G *with* $|P| = p = |Q|$*, then either* $P = Q$ *or* $P \cap Q = \{e\}$*.*

Proof. If $P \cap Q \neq \{e\}$ then choose $x \in P \cap Q$ with $x \neq e$. By the previous theorem, x generates both P and Q, so $P = \langle x \rangle = Q$. □

Now some other simple general consequences of Lagrange's Theorem.

Proposition 12.6. *Let* G *be a group and* H,K *two finite subgroups of* G *with* $|H| = m$, $|K| = n$ *and* $\text{hcf}(m, n) = 1$. *Then* $H \cap K = \{e\}$.

Proof. Recall that the intersection of two subgroups is iself a subgroup, so that $I = H \cap K$ is a subgroup both of H and of K. Since it's a subgroup of H, Lagrange's Theorem implies that $|I|$ divides $m = |H|$. But similarly $|I|$ divides $n = |K|$. So since $\text{hcf}(m, n) = 1$, $|I| = 1$ and so $I = \{e\}$. □

Theorem 12.7. *Let* G *be a group with* $|G| = 4$. *Then either* G *is cyclic or* G *is isomorphic to the Klein* 4*-group* $C_2 \times C_2$. *In particular there are just two non-isomorphic groups of order* 4, *both abelian.*

Proof. By Corollary 12.1 the order of any element of G divides 4, and so must be 1, 2 or 4.

If G has an element of order 4 then it is cyclic.

If not, it must have one element (the identity e) of order 1 and three elements a, b, c of order 2. So $a^{-1} = a$, $b^{-1} = b$ and $c^{-1} = c$.

Consider which element is ab. If $ab = e$ then $b = a^{-1}$, which is false, since $a^{-1} = a$. If $ab = a$ then $b = e$, which is also false. If $ab = b$ then $a = e$, which is also false. So $ab = c$.

Similarly $ba = c$, $ac = b = ca$ and $bc = a = cb$, and G is isomorphic to the Klein 4-group. □

We'll finish this section with some other results about groups of small order that we won't prove. These are easier to prove with a bit more theory, which will all proved in the third year Group Theory unit.

Theorem 12.8. *Let* p *be an odd prime. Then every group of order* $2p$ *is either cyclic or isomorphic to the dihedral group* D_{2p}.

Theorem 12.9. *Let* p *be a prime. Every group of order* p^2 *is either cyclic or isomorphic to* $C_p \times C_p$ *(and so in particular is abelian).*

Howeer there are non-abelian groups of order p^3 for every prime p. The dihedral group D_8 is one example for $p = 2$.

Theorem 12.10. *There are five groups of order* 8 *up to isomorphism. Three,* C_8, $C_4 \times C_2$ *and* $C_2 \times C_2 \times C_2$, *are abelian, and two, the dihedral group* D_8 *and another group* Q_8 *called the* **quaternion group** *are non-abelian.*

The first few orders not dealt with by the general theorems above are 12, 15, 16 and 18. It turns out that are five non-isomorphic groups of order 12, every group of order

15 is cyclic, there are fourteen non-isomorphic groups of order 16, and five of order 18.

The number of non-isomorphic groups of order 2^n grows very quickly with n. There are $49,487,365,422$ (nearly fifty billion) non-isomorphic groups of order $1024 = 2^{10}$.

13. Symmetric groups and cycles

We have already met symmetric groups, but not with that name. A symmetric group is just the group of all permutations of a set. We'll only really consider finite sets, although the definition makes sense for any set.

Definition 13.1. (1) Let X be a set. The **symmetric group** on X is the group $S(X)$ of all permutations of X (i.e., bijective functions $f : X \to X$), with composition as the group operation.

(2) The **symmetric group** S_n **of degree** n is the group of all permutations of the set $\{1, 2, \ldots, n\}$ of n elements.

Any other set of n elements would do in place of $\{1, 2, \ldots, n\}$. The group we'd get would be isomorphic to S_n.

Recall from Section 1 that our convention for composing permutations is that fg means "do g first, and then f".

Proposition 13.1. $|S_n| = n!$.

Proof. We'll count the permutations of $\{1, 2, \ldots, n\}$. Let $f \in S_n$. Since $f(1)$ can be any of the elements $1, 2, \ldots, n$, there are n possibilities for $f(1)$. For each of these, there are $n-1$ possibilities for $f(2)$, since it can be any of the elements $1, 2, \ldots, n$ except for $f(1)$. Given $f(1), f(2)$, there are $n-2$ possibilities for $f(3)$, since it can be any of the elements $1, 2, \ldots, n$ except for $f(1)$ and $f(2)$. And so on. So in total there are

$$n(n-1)(n-2)\ldots 2.1 = n!$$

permutations of $\{1, 2, \ldots, n\}$. □

Let's think of ways of describing permutations. Of course, we could just say what $f(i)$ is for each value of i, and so, for example, refer to the element f of S_6 with $f(1) = 3$, $f(2) = 6$, $f(3) = 1$, $f(4) = 4$, $f(5) = 2$ and $f(6) = 5$.

This is quite hard to read, and one easy way to set out the information in a more easily readable form is to use a "double row" notation with $1, 2, \ldots, n$ along the top row, and $f(1), f(2), \ldots, f(n)$ along the bottom row.

For example, if f is the element of S_6 described above, then we could write

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 4 & 2 & 5 \end{pmatrix}.$$

But there's an even more compact method, that is also much more convenient for understanding group theoretic aspects of permutations.

Definition 13.2. Let k and n be positive integers with $k \leq n$. A k**-cycle** f in S_n is a permutation of the following form. There are k distinct elements $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$,

$$f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_{k-1}) = i_k, f(i_k) = i_1$$

and $f(i) = i$ for $i \notin \{i_1, i_2, \ldots, i_k\}$. (So f "cycles" the elements $i_1, i_2, \ldots, i_k$ and leaves other elements unmoved.)

Such an f is denoted by $f = (i_1, i_2, \ldots, i_k)$.

We call k the **length** of this cycle.

Example 13.1. In S_8, the 6-cycle

$$g = (2, 7, 8, 5, 6, 3)$$

has

$$g(2) = 7, g(7) = 8, g(8) = 5, g(5) = 6, g(6) = 3, g(3) = 2, g(1) = 1 \text{ and } g(4) = 4,$$

or, written in double row notation,

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

The notation $(2, 7, 8, 5, 6, 3)$ would also denote an element of S_9 with $g(9) = 9$, so this notation doesn't specify which symmetric group we're looking at, although that is rarely a problem.

Note that the 6-cycle $(7, 8, 5, 6, 3, 2)$ is exactly the same permutation as g, so the same cycle can be written in different ways (in fact, a k-cycle can be written in k different ways, as we can choose to start the cycle with any of the k elements $i_1, i_2, \ldots, i_k$.

It is clear that if we repeat a k-cycle $(i_1, i_2, \ldots, i_k)$ k times, each element i_j is sent back to itself (and if we repeat it $l < k$ times, then i_1 is sent to $i_{l+1} \neq i_1$. In group-theoretic language:

Proposition 13.2. *The order of a k-cycle in the symmetric group S_n is k.*

Remark 13.1. We'll allow $k = 1$, but every 1-cycle (i_1) is just the identity permutation, since it send i_1 to i_1 and every $i \neq i_1$ to i, so we'll rarely bother to write down 1-cycles.

Definition 13.3. A **transposition** is another name for a 2-cycle. So this is just a permutation that swaps two elements and leaves all other elements unmoved.

Of course, not every permutation is a cycle. For example, the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 4 & 2 & 5 \end{pmatrix}$$

that we used as an example earlier is not. However, we can write it as a composition

$$f = (1, 3)(2, 6, 5)$$

of two cycles. These two cycles are "disjoint" in the sense that they move disjoint set of elements $\{1, 3\}$ and $\{2, 5, 6\}$, and this means that it makes no difference which of the two cycles we apply first. So also

$$f = (2, 6, 5)(1, 3).$$

Definition 13.4. A set of cycles in S_n is **disjoint** if no element of $\{1, 2, \ldots, n\}$ is moved by more than one of the cycles.

Theorem 13.3. *Every element of S_n is a product of disjoint cycles.*

Proof. Rather than giving a formal proof, we'll give a method to write a permutation f as such a product.

We'll write down a set of disjoint cycles by considering repeatedly applying f to elemens of $\{1, 2, \ldots, n\}$, starting with the smallest elements.

So we start with 1, and consider $f(1), f^2(1), \ldots$ until we reach an element $f^k(1)$ that we have already reached. The first time this happens must be with $f^k(1) = 1$, since if $f^k(1) = f^l(1)$ for $0 < l < k$ then $f^{k-1}(1) = f^{l-1}(1)$, and so we'd have repeated the element $f^{l-1}(1)$ earlier. So we have a cycle

$$(1, f(1), f^2(1), \ldots, f^k(1).$$

Now we start again with the smallest number i that is not involved in any of the cycles we've already written down, and get another cycle $(i, f(i), \ldots, f^s(i))$ for some s.

We keep repeating until we've dealt with all the elements of $\{1, 2, \ldots, n\}$. □

This will probably be clearer if we look at an example.

Example 13.2. Consider the element

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

of S_9 written in double row notation. To write this as a product of disjoint cycles, we start with 1, and calculate

$$f(1) = 2, f(2) = 5, f(5) = 7, f(7) = 3, f(3) = 1,$$

so we have a 5-cycle $(1, 2, 5, 7, 3)$.

The smallest number we haven't yet dealt with is 4, and

$$f(4) = 9, f(9) = 8, f(8) = 4,$$

so we have a 3-cycle $(4, 9, 8)$.

The only number we haven't dealt with is 6, and

$$f(6) = 6,$$

so finally we have a 1-cycle (6).

So

$$f = (1, 2, 5, 7, 3)(4, 9, 8)(6)$$

as a product of disjoint cycles. Since 1-cycles are just the identity permutation, we can (and usually will) leave them out, and so we can write

$$f = (1, 2, 5, 7, 3)(4, 9, 8).$$

Since the order in which we apply disjoint permutations doesn't matter, we could write the cycles in a different order, or we could start each cycle at a different point. So, for example,

$$f = (9, 8, 4)(5, 7, 3, 1, 2)$$

is another way of writing the same permutation as a product of disjoint cycles.

It's very easy to read off the product of permutations written in disjoint cycle notation, just by using the method in the proof of Theorem 13.3.

Example 13.3. Let

$$f = (1, 5, 3, 4)(2, 6, 7)$$

and

$$g = (3, 8, 1, 2, 5)(4, 3)$$

be elements of S_8 written in disjoint cycle notation. Let's calculate fg and gf.

$$fg = (1, 5, 3, 4)(2, 6, 7)(3, 8, 1, 2, 5)(4, 3),$$

but of course these arre not *disjoint* cycles. So we start with 1 and calculate where it is sent by perfoming the permutation fg repeatedly:

- 1 is not moved by $(4, 3)$, it's sent to 2 by $(3, 8, 1, 2, 5)$, which is sent to 6 by $(2, 6, 7)$, which is not moved by $(1, 5, 3, 4)$. So $fg(1) = 6$.
- 6 is not moved by $(4, 3)$ or $(3, 8, 1, 2, 5)$. It is sent to 7 by $(2, 6, 7)$, which is not moved by $(1, 5, 3, 4)$. So $fg(6) = 7$.
- 7 is not moved by $(4, 3)$ or $(3, 8, 1, 2, 5)$. It is sent to 2 by $(2, 6, 7)$, which is not moed by $(1, 5, 3, 4)$. So $fg(7) = 2$.
- 2 is not moved by $(4, 3)$. It is sent to 5 by $(3, 8, 1, 2, 5)$, which is not moved by $(2, 6, 7)$ and is sent to 3 by $(1, 5, 3, 4)$. So $fg(2) = 3$.
- 3 is sent to 4 by $(4, 3)$, which is not moved by $(3, 8, 1, 2, 5)$ or $(2, 6, 7)$, and sent to 1 by $(1, 5, 3, 4)$. So $fg(3) = 1$.
- So we've completed our first cycle $(1, 6, 7, 2, 3)$.
- 4 is sent to 3 by $(4, 3)$, which is sent to 8 by $(3, 8, 1, 2, 5)$, which is not moved by $(2, 6, 7)$ or $(1, 5, 3, 4)$. So $fg(4) = 8$.
- 8 is not moved by $(4, 3)$. It is sent to 1 by $(3, 8, 1, 2, 5)$, which is not moved by $(2, 6, 7)$ and sent to 5 by $(1, 5, 3, 4)$. So $fg(8) = 5$.
- 5 is not moved by $(4, 3)$, it's sent to 3 by $(3, 8, 1, 2, 5)$, which is not moved by $(2, 6, 7)$ and sent to 4 by $(1, 5, 3, 4)$. So $fg(5) = 4$.
- So we've completed another cycle $(4, 8, 5)$.

- We've now dealt with all the numbers from 1 to 8, so $fg = (1,6,7,2,3)(4,8,5)$ as a product of disjoint cycles.

Similarly,

$$gf = (3,8,1,2,5)(4,3)(1,5,3,4)(2,6,7) = (1,3,8)(2,6,7,5,4)$$

as a product of disjoint cycles.

Example 13.4. It is easy to write down the inverse of a permutation written as a product of disjoint cycles. Just write the permutation backwards. For example, if

$$f = (1,4,3,5,7)(2,6,8)$$

then

$$f^{-1} = (8,6,2)(7,5,3,4,1).$$

Of course, we have a choice of which order to take the cycles, and where to start each cycle, and if we carried out the method in the proof of Theorem 13.3 then we'd get the alternative representation

$$f^{-1} = (1,7,5,3,4)(2,8,6).$$

One benefit of disjoint cycle notation is that it makes it easy to calculate the order of a permutation.

Theorem 13.4. *If* f *is the product of disjoint cycles of lengths* $k_1, k_2, \ldots, k_r$*, then*

$$\mathrm{ord}(f) = \mathrm{lcm}(k_1, k_2, \ldots, k_r).$$

Proof. Consider when f^k is the identity permutation. For $f^k(j_i) = j_i$ when j_i is one of the numbers involved in the k_i-cycle, we need k_i to divide k. But if k_i divides k for all i, then this applies to all the numbers moved by f. So the smallest such k is the lowest common multiple of $k_1, \ldots, k_r$. □

Example 13.5. The order of the permutation $(1,6,7,2,3)(4,8,5)$ from a previous example is $\mathrm{lcm}(5,3) = 15$. Notice that if we write this permutation as

$$(1,5,3,4)(2,6,7)(3,8,1,2,5)(4,3),$$

using cycles that are not disjoint, it is much less clear what the order is, and it is definitely not the lowest common multiple of the cycle lengths.

14. TRANSPOSITIONS AND ALTERNATING GROUPS

Recall that a "transposition" is just another name for a 2-cycle.

Theorem 14.1. *Every permutation $f \in S_n$ is a product of transpositions.*

Remark 14.1. We'll interpret the product of zero transpositions to mean the identity permutation. Alternatively, if $n > 1$, we have $e = (1,2)(1,2)$ as a product of two transpositions.

Proof of Theorem 14.1. Let $f \in S_n$, and let m be the number of elements i of $\{1, 2, \ldots, n\}$ that are moved by f: i.e., such that $f(i) \neq i$. We'll prove the theorem by induction on m.

In the base case $m = 0$, f is the identity permutation, which is a product of zero transpositions.

Suppose inductively that every permutation that moves fewer than m elements is a product of transpositions, and let i be one of the m elements moved by f. If τ is the transposition $(i, f(i))$ swapping i and $f(i)$, then $f\tau$ sends $f(i)$ to $f(i)$, and so moves fewer than m elements. So by induction $f\tau$ can be written as a product

$$f\tau = \tau_1\tau_2 \ldots \tau_k$$

of transpositions. Since $\tau^{-1} = \tau$, we get that

$$f = \tau_1\tau_2 \ldots \tau_k\tau$$

is a product of transpositions. □

Remark 14.2. The idea of the proof is probably exactly how you would put a sequence of elements in the right order by successively swapping elements to put them in the right place one by one. The number of transpositions needed if f moves $m > 0$ elements is at most $m - 1$.

Let's look explicitly at the case where f is a cycle.

Proposition 14.2. *For $k > 1$, a k-cycle is a product of $k - 1$ transpositions.*

Proof. Just notice that

$$(1, 2, \ldots, k) = (1,2)(2,3)\ldots(k-1,k).$$

□

Remark 14.3. Another way to prove Theorem 14.1 would be to use Proposition 14.2 together with the fact that every permutation can be written as a product of (disjoint) cycles.

Definition 14.1. Let $f \in S_n$. We say that f is an **even permutation** if it can be written as a product of an even number of transpositions, and an **odd permutation** if it can be written as a product of an odd number of transpositions.

Theorem 14.3. *Every $f \in S_n$ is either even or odd, but not both.*

Proof. [This proof uses some linear algebra, and you won't be asked for it in the exam, although you are expected to know and understand the statement of the theorem.]

By Theorem 14.1, f is a product of transpositions, so according to the definition is either even or odd, So we just need to show that it can't be written as a product both of an even number and of an odd number of transpositions.

Consider the $n \times n$ identity matrix I_n, and permute the rows using the permutation f; i.e., replace the ith row with the $f(i)$th row for each i. Consider the determinant of the matrix A obtained.

Since $\det(I_n) = 1$, and swapping two rows of a square matrix multiplies the determinant by -1, permuting the rows by an even permutation multiplies the determinant by $+1$ and permuting by an odd permutation multiplies the determinant by -1. So $\det(A) = 1$ or $\det(A) = -1$ according to whether f is even or odd. In particular, both can't happen. □

Remark 14.4. Another way to prove this is to consider the number of pairs of elements $i, j \in \{1, 2, \ldots, n\}$ such that $i < j$ but $f(i) > f(j)$, and show that the number of such pairs is even/odd according to whether f is even/odd.

The following is immediate from the definition of even/odd.

Proposition 14.4. *Let $f, g \in S_n$. Then fg is even if f and g are either both even or both odd. If one of f and g is even and one odd, then fg is odd.*

Proposition 14.5. *A k-cycle is even if k is odd, and odd if k is even.*

Proof. This follows immediately from Proposition 14.2. □

The last two Propositions make it easy to see whether a permutation written as a product of cycles (disjoint or otherwise) is even or odd.

Proposition 14.6. *Let*

$$f = \sigma_1 \sigma_2 \ldots \sigma_k$$

be a product of cycles σ_i. Then f is even if the number of σ_i of even length is even, and odd if the number of cycles of even length is odd.

Proof. Just use the fact that cycles of odd length are even and cycles of even length are odd, together with Proposition 14.4. □

Example 14.1. $(1,3)(2,3,4)(1,4,6,2)(1,3,4,5)$ is odd, since three (an odd number) of the cycles have even length. Notice that if we write this as a product of *disjoint* cycles, we get $(1,4,5,2,3,6)$, which also has an odd number (one) of cycles of even length.

Note that if we use Proposition 14.2 to write the cycles as products of transpositions in each of these representations of the same permutation, we get

$$(1,3)(2,3,4)(1,4,6,2)(1,3,4,5) = (1,3)(2,3)(3,4)(1,4)(4,6)(6,2)(1,3)(3,4)(4,5),$$

a product of nine transpositions, and

$$(1,4,5,2,3,6) = (1,4)(4,5)(5,2)(2,3)(3,6),$$

a product of five transpositions. So it is certainly possible to write a given permutation in many different ways as the product of different numbers of transpositions, but the number will either always be odd or always be even.

We can interpret much of what we've proved in terms of a subgroup.

Proposition 14.7. *The set of even permutations in S_n is a subgroup of S_n.*

Proof. It contains the identity element (the product of zero transpositions), it is closed by Proposition 14.4, and it is closed under taking inverses, since if

$$f = \tau_1\tau_2\dots\tau_{2k}$$

as a product of an even number of transpositions, then

$$f^{-1} = \tau_{2k}\dots\tau_2\tau_1,$$

since $\tau_i^{-1} = \tau_i$, and so f^{-1} is a product of an even number of transpositions. □

Definition 14.2. The **alternating group** A_n is the subgroup of S_n consisting of all the even permutations.

Example 14.2. S_4 has $4! = 24$ elements. The even ones are the identity e, the 3-cycles (of which there are eight), and the three elements $(1,2)(3,4)$, $(1,3)(2,4)$ and $(1,4)(2,3)$ that are products of two disjoint transpositions. So there are 12 even permutations in S_4. The odd permutations are the transpositions (of which there are six) and the 4-cycles (of which there are also six). So there are 12 odd permutations in S_4. Note that there are equal numbers of odd and even permutations.

Theorem 14.8. *If $n > 1$ then $|A_n| = \frac{n!}{2} = \frac{1}{2}|S_n|$.*

Proof. Let τ be the transposition $(1,2)$. For $f \in S_n$, f is even if and only if $f\tau$ is odd, so $f \mapsto f\tau$ is a bijection from the set of even permutations to the set of odd permutations (with its inverse also given by $g \mapsto g\tau$). So exactly half the elements of S_n are in A_n. □

Example 14.3. A_4 is a group of order $12 = \frac{4!}{2}$. It is non-abelian, since (for example) $f = (1,2,3)$ and $g = (2,3,4)$ are both elements of A_4, but

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

whereas

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

so $fg \neq gf$.

We already know one non-abelian group of order 12: namely, the dihedral group D_{12}. We can easily see that $A_4 \ncong D_{12}$, since D_{12} contains the element a of order 6, but A_4 contains no elements of order 6, since the 3-cycles have order 3 and the products of disjoint transpositions have order 2.

There is also one other non-abelian group of order 12 that is isomorphic to neither A_4 nor D_{12}, making a total of 5 non-isomorphic groups of order 12 when we include the abelian groups C_{12} and $C_2 \times C_6$.

The alternating group A_4 is the smallest counterexample to the "converse" of Lagrange's theorem. Despite the fact that 6 divides the order of A_4, it doesn't have a subgroup of order 6.

Proposition 14.9. *A_4 has no subgroup of order 6.*

Sketch of proof. Suppose $H \leq A_4$ with $|H| = 6$. Then H can't be cyclic, since A_4 has no elements of order 6. But then H must be isomorphic to D_6, since there are only two groups of order 6, C_{12} and D_6, up to isomorphism. Since D_6 has three elements of order 2, and the only elements of A_4 with order 2 are $(1,2)(3,4)$, $(1,3)(2,4)$ and $(1,4)(2,3)$, these must all be in H. But it is easy to check that

$$K = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

is a subgroup of A_4, and so must be a subgroup of H, contradicting Lagrange's Theorem since 4 does not divide $|H| = 6$. □

15. HOMOMORPHISMS AND NORMAL SUBGROUPS

A group homomorphism is a function between two groups that links the two group operations in the following way.

Definition 15.1. Let $(G, *)$ and $(H, \bullet)$ be groups. A group **homomorphism** $\varphi : G \to H$ is a function such that

$$\varphi(x * y) = \varphi(x) \bullet \varphi(y)$$

for all $x, y \in G$.

Example 15.1. An isomorphism is a homomorphism. The difference is that we don't require a homomorphism to be bijective. If it is, then it is an isomorphism.

Remark 15.1. If the groups G and H are written multiplicatively, then $\varphi : G \to H$ is a homomorphism if

$$\varphi(xy) = \varphi(x)\varphi(y)$$

for all $x, y \in G$. But it should be noted that on the left hand side of that equation we multiply x and y in G, but on the right hand side we multiply $\varphi(x)$ and $\varphi(y)$ in H, so this still links the group operations of different groups.

Remark 15.2. If you are doing Linear Algebra, then you may find it helpful to note a similarity between the definitions of a group homomorphism and a linear map. These are both functions that "commute with the operations" in the sense that the definition of a homomorphism says that multiplying two elements and then applying the homomorphism gives the same as applying the homomorphism to the two elements and then multiplying the resultan elements, and the definition of a linear map says the same for the operations of addition and multiplication by scalars in place of the group operation. In fact, many of the basic facts about homomorphisms are very similar to basic facts about linear maps, usually with pretty much the same proof.

Example 15.2. If G and H are groups and e_H is the identity element of H, the function $\varphi : G \to H$ given by

$$\varphi(x) = e_H$$

for all $x \in G$ is a homomorphism (the **trivial homomorphism**).

Example 15.3. If $H \leq G$ are groups, then the inclusion map $i : H \to G$ given by

$$i(x) = x \in G$$

for all $x \in H$ is a homomorphism. This is injective but not surjective (unless $H = G$).

The existence of an isomorphism between two groups implies that the two groups have the same abstract structure, as we have seen. The existence of a homomorphism doesn't: indeed, the example of the trivial homomorphism shows that there is a homomorphism between *any* two groups. However, (non-trivial) homomorphisms from a group G to a more familiar group H can still be very useful tools to understand G.

Proposition 15.1. *Let H and K be groups, and let $H \times K$ be the direct product. Then there are homomorphisms*

(1) $i_H : H \to H \times K$ *with* $i_H(x) = (x, e_K)$ *for* $x \in H$.
(2) $i_k : K \to H \times K$ *with* $i_K(y) = (e_H, y)$ *for* $y \in K$.
(3) $\pi_H : H \times K \to H$ *with* $\pi_H(x, y) = x$ *for* $x \in H$, $y \in K$.
(4) $\pi_K : H \times K \to K$ *with* $\pi_K(x, y) = y$ *for* $x \in H$, $y \in K$.

Proof. i_H is a homomorphism since, for $x, x' \in H$,

$$i_H(xx') = (xx', e_K) = (x, e_K)(x', e_K) = i_H(x)i_H(x').$$

π_H is a homomorphism since, for $x, x' \in H$ and $yy, y' \in K$,

$$\pi_H\left((x, y)(x', y')\right) = \pi_H(xx', yy') = xx' = \pi_H(x, y)\pi_H(x', y').$$

The proofs for i_K and π_K are similar. □

Lemma 15.2. *Let $\varphi : G \to H$ be a homomorphism, let e_G and e_H be the identity elements of G and H respectively, and let $x \in G$. Then*

(1) $\varphi(e_G) = e_H$,
(2) $\varphi(x^{-1}) = \varphi(x)^{-1}$,
(3) $\varphi(x^i) = \varphi(x)^i$ *for any* $i \in \mathbb{Z}$.

Proof.
(1) $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$, so by uniqueness of the identity $\varphi(e_G) = e_H$.
(2) $e_H = \varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, so by uniqueness of inverses $\varphi(x^{-1}) = \varphi(x)^{-1}$.
(3) This is true for positive i by a simple induction (it is true for $i = 1$, and if it is true for $i = k$ then

$$\varphi(x^{k+1}) = \varphi(x^k)\varphi(x) = \varphi(x)^k\varphi(x) = \varphi(x)^{k+1},$$

so it is true for $i = k + 1$). Then by (2) it is true for negative i, and by (1) it is true for $i = 0$.

□

Definition 15.2. Let $\varphi : G \to H$ be a homomorphism and e_H the identity element of H. The **kernel** of φ is

$$\ker(\varphi) = \{x \in G : \varphi(x) = e_H\} \subseteq G,$$

and the **image** of φ is

$$\mathrm{im}(\varphi) = \{\varphi(x) : x \in G\} \subseteq H.$$

Theorem 15.3. *If $\varphi : G \to H$ is a homomorphism, then $\ker(\varphi)$ is a subgroup of G and $\mathrm{im}(\varphi)$ is a subgroup of H.*

Proof. Since, by Lemma 15.2, $\varphi(e_G) = e_H$, $e_G \in \ker(\varphi)$.

If $x, x' \in \ker(\varphi)$ then

$$\varphi(xx') = \varphi(x)\varphi(x') = e_H e_H = e_H,$$

so $xx' \in \ker(\varphi)$, and so $\ker(\varphi)$ is closed under multiplication.

If $x \in \ker(\varphi)$ then by Lemma 15.2 $\varphi(x^{-1}) = \varphi(x)^{-1} = e_H^{-1} = e_H$, so $x^{-1} \in \ker(\varphi)$, and so $\ker(\varphi)$ is closed under taking inverses.

So $\ker(\varphi)$ is a subgroup of G.

$e_H = \varphi(e_G)$ by Lemma 15.2, so $e_H \in \mathrm{im}(\varphi)$.

If $y, y' \in \mathrm{im}(\varphi)$ then $y = \varphi(x)$ and $y' = \varphi(x')$ for some $x, x' \in G$, and so

$$yy' = \varphi(x)\varphi(x') = \varphi(xx')$$

is in $\mathrm{im}(\varphi)$, and so $\mathrm{im}(\varphi)$ is closed under multiplication.

If $y \in \mathrm{im}(\varphi)$ then $y = \varphi(x)$ for some $x \in G$, and by Lemma 15.2

$$y^{-1} = \varphi(x)^{-1} = \varphi(x^{-1}),$$

so $y^{-1} \in \mathrm{im}(\varphi)$, and so $\mathrm{im}(\varphi)$ is closed under taking inverses.

So $\mathrm{im}(\varphi)$ is a subgroup of H. □

Example 15.4. Let D_{2n} be the dihedral group of order n, let $H = (\{1, -1\}, \times)$ and define $\varphi : D_{2n} \to H$ by

$$\varphi(x) = \begin{cases} 1 & \text{if } x \text{ is a rotation} \\ -1 & \text{if } x \text{ is a reflection.} \end{cases}$$

Then it is easy to check that φ is a homomorphism. $\ker(\varphi) = \langle a \rangle$ is the subgroup containing all rotations, and of course φ is surjective, so $\mathrm{im}(\varphi) = H$.

Example 15.5. Let S_n be the symmetric group of degree n, let $H = (\{1, -1\}, \times)$ and define $\varphi : S_n \to H$ by

$$\varphi(x) = \begin{cases} 1 & \text{if } x \text{ is an even permutation} \\ -1 & \text{if } x \text{ is an odd permutation.} \end{cases}$$

Then it is easy to check that φ is a homomorphism. $\ker(\varphi)$ is the alternating group A_n, and if $n > 1$ then φ is surjective, and so $\mathrm{im}(\varphi) = H$.

Example 15.6. Example 15.4 shows that $\langle a \rangle$ is the kernel of a homomorphism from D_{2n} to another group. What about other subgroups, such as $\langle b \rangle$?

Suppose $\varphi : D_{2n} \to H$ is a homomorphism with $b \in \ker \varphi$. Then

$$\varphi(aba^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1} = \varphi(a)e_H\varphi(a)^{-1} = e_H,$$

so aba^{-1}, which is equal to a^2b, must also be in $\ker(\varphi)$. So if $n > 2$ (so that $a^2b \neq b$) then $\langle b \rangle$ cannot be the kernel of a homomorphism. This motivates the following definition.

Definition 15.3. Let G be a group. A **normal subgroup** of G is a subgroup $N \leq G$ such that $gxg^{-1} \in N$ for every $g \in G$ and $x \in N$. The notation $N \trianglelefteq G$ is used to mean that N is a normal subgroup of G, or $N \triangleleft G$ if we want to specify that $N \neq G$.

We can generalize the argument in the last example:

Theorem 15.4. *Let* $\varphi : G \to H$ *be a homomorphism. Then* $\ker(\varphi) \trianglelefteq G$.

Proof. We have already proved that $\ker(\varphi)$ is a subgroup of G.

Let $g \in G$ and $x \in \ker(\varphi)$. Then

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)e_H\varphi(g)^{-1} = e_H,$$

so $gxg^{-1} \in \ker(\varphi)$, and so $\ker(\varphi)$ is a normal subgroup of G. □

Remark 15.3. In fact, finding a homomorphism φ such that $N = \ker(\varphi)$ is often the easiest way to prove that N is a normal subgroup of G.

Example 15.7. $H = \langle b \rangle$ is not a normal subgroup of D_{2n} if $n > 2$, since $aba^{-1} \notin H$. However, $K = \langle a \rangle$ is a normal subgroup since we showed in Example 15.4 that it is the kernel of a homomorphism.

Similarly, the alternating group A_n is a normal subgroup of S_n, as we showed in Example 15.5 that it is the kernel of a homomorphism.

Proposition 15.5. *If* G *is an abelian group then every subgroup of* G *is normal.*

Proof. Let $N \subseteq G$, $g \in G$ and $x \in N$. Then if G is abelian, $gxg^{-1} = x \in N$, and so $N \trianglelefteq G$. □

There are some other ways to formulate the definition of a normal subgroup. Recall the definition of the left coset $gN = \{gx : x \in N\}$ and right coset $Ng = \{xg : x \in N\}$ for $N \leq G$ and $g \in G$. Using similar notation we define

$$gNg^{-1} = \left\{gxg^{-1} : x \in N\right\}.$$

Proposition 15.6. *Let* G *be a group and* $N \leq G$*. The following are equivalent.*

(1) $N \trianglelefteq G$.
(2) $gNg^{-1} = N$ *for all* $g \in G$.
(3) $gN = Ng$ *for all* $g \in G$.

Proof. (1) $\Rightarrow$ (2): Suppose $N \trianglelefteq G$ and $g \in G$. The definition of "normal subgroup" says that $gNg^{-1} \subseteq N$ for all $g \in G$. But applying this to g^{-1} this in particular implies that $g^{-1}Ng \subseteq N$ and so

$$x \in N \Rightarrow g^{-1}xg \in N \Rightarrow x = g(g^{-1}xg)g^{-1} \in gNg^{-1}.$$

(2) $\Rightarrow$ (1) is trivial.

If $gNg^{-1} = N$ then for $gx \in gN$, $gx = (gxg^{-1})g \in Ng$ so $gN \subseteq Ng$ and similarly $Ng \subseteq gN$, so (2) $\Rightarrow$ (3).

If $gN = Ng$ and $x \in N$, then $gx \in Ng$, so $gx = yg$ for some $y \in N$, and so $gxg^{-1} = ygg^{-1} = y \in N$, so $gNg^{-1} \subseteq N$, so (3) $\Rightarrow$ (1). □

Remark 15.4. This tells us that a subgroup is normal if and only if its left cosets are the same as its right cosets. Let's look at how this works in the example of $N = \langle a \rangle \trianglelefteq D_6$ and the left and right cosets bN and Nb.

Since $N = \{e, a, a^2\}$,

$$bN = \{be, ba, ba^2\} = \{b, ab^2, ab\}$$

and

$$Nb = \{eb, ab, a^2b\}.$$

So as expected since $N \trianglelefteq D_6$, $bN = Nb$.

However, notice that this is **NOT** saying that $bx = xb$ for every $x \in N$. Indeed, in this example $ab \neq ba = a^2b$. For $x = a$ it *is* true that xb is in bN, but it is equal to by for an element $y \in N$ that is different from x.

16. QUOTIENT GROUPS

We've seen that the kernel of a homomorphism is always a normal subgroup. Now we'll look at an important construction that shows that every normal subgroup is the kernel of some homomorphism.

Let's start with a familiar example, $(\mathbb{Z}/n\mathbb{Z}, +)$. We can think of this as being constructed from the group $(\mathbb{Z}, +)$ and the subgroup $n\mathbb{Z} = \{ns : s \in \mathbb{Z}\}$ as follows:

We regard elements of $\mathbb{Z}$ (i.e., integers) as "equivalent" if their difference is in $n\mathbb{Z}$ (i.e., if they are congruent $\pmod n$). Then we form a new group $\mathbb{Z}/n\mathbb{Z}$ whose elements are equivalence classes $[s]$ of elements of $\mathbb{Z}$ and with group operation $[s][t] = [s + t]$, which we check is well-defined.

In fact, we can do exactly the same construction for any abelian group G and subgroup H, but if G is not abelian, then we have to be more careful about what the "difference" between two elements x and y means: do we mean xy^{-1} or $y^{-1}x$, which may be different? This is why it turns out to be important that our subgroup is normal.

Let's look at a simple example, to point out the problems.

Example 16.1.
- Let $G = D_6$ and let N be the (normal) subgroup $\langle a \rangle$. Then there are two left cosets N (consisting of the rotations) and bN (consisting of the reflections). If we compose two rotations we get a rotation; if we compose two reflections we get a rotation, and if we compose (in either order) a rotation and a reflection then we get a reflection. So if we want to know which coset xy is in, then we only need to know which cosets x and y are in.
- Let $G = D_6$ and let H be the (non-normal) subgroup $\langle b \rangle$. Then there are three left cosets $H = \{e, b\}$, $aH = \{a, ab\}$ and $a^2H = \{a^2, a^2b\}$. Observe what happens if we multiply two elements $x \in H$ and $y \in aH$: if $x = e$ and $y = a$ then $xy = a$, which is in the coset aH, but if $x = b$ and $y = ab$ then $xy = bab = a^2$, which is in the coset a^2H. So the coset that contains xy does *not* depend only on which cosets contain x and y.

Let G be a group and $N \trianglelefteq G$ a normal subgroup. Remember that this means that the left coset xN and right coset Nx are the same for every $x \in N$. To simplify the notation, and point out the analogy with modular arithmetic, we'll use the notation

$$[x] = xN = Nx$$

for the cosets.

Lemma 16.1. *If* $x, y \in G$, *then* $[xy]$ *depends only on* $[x]$ *and* $[y]$.

Proof. Let $xn \in [x]$ and $yn' \in [y]$. Then $xnyn' = xy(y^{-1}ny)n'$, which is in xyN since N is normal and so $y^{-1}ny \in N$. □

Definition 16.1. If G is a group and $N \trianglelefteq G$ a normal subgroup. The **quotient group** G/N is the set of cosets of N in G, with the binary operation (written multiplicatively)

$$[x][y] = [xy],$$

for $x, y \in G$.

By the previous lemma, this binary operation is well-defined. But of course we need to check that this is a group.

Theorem 16.2. *If $N \trianglelefteq G$, then G/N is a group.*

Proof. Since

$$([x][y])[z] = [xy][z] = [xyz] = [x][yz] = [x]([y][z]),$$

for any $x, y, z \in G$, it is associative.

Since

$$[e][x] = [ex] = [x] = [xe] = [x][e]$$

for any $x \in G$, $[e]$ is an identity element.

Since

$$[x][x^{-1}] = [xx^{-1}] = [e] = [x^{-1}x] = [x^{-1}][x]$$

for any $x \in G$, $[x^{-1}]$ is an inverse to $[x]$. □

There is a natural function $\pi : G \to G/N$ defined by sending an element of G to the coset that contains it: $\pi(x) = [x]$.

Proposition 16.3. *$\pi : G \to G/N$ is a surjective homomorphism with $\ker(\pi) = N$.*

Proof. Clearly π is surjective, since every element of G/N is of the form $[x] = \pi(x)$ for some $x \in G$.

If $x, y \in G$ then

$$\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y),$$

so π is a homomorphism.

Since, for $x \in G$,

$$x \in \ker(\pi) \Leftrightarrow [x] = [e] = N \Leftrightarrow x \in N,$$

$\ker(\pi) = N$. □

In fact, we'll see later that this Proposition characterizes G/N up to isomorphism. It's really because of this property that quotient groups are useful and important, and the details of the construction using cosets are only important in order to prove that there *is* a group G/N with this property.

17. The Homomorphism Theorem

In this section we'll prove an important theorem that gives a link between the kernel and image of a group homomorphism. This is variously known as the "Homomorphism Theorem" or the "First Isomorphism Theorem" (although the second name is also sometimes used for a different theorem).

Recall that if $\varphi : G \to H$ is a group homomorphism, then $\ker(\varphi)$ is a normal subgroup of G, and so it makes sense to form the quotient group $G/\ker(\varphi)$.

Theorem 17.1 (Homomorphism Theorem)**.** *Let $\varphi : G \to H$ be a group homomorphism. Then the quotient group $G/\ker(\varphi)$ is isomorphic to $\mathrm{im}(\varphi)$.*

Proof. We'll prove this by constructing an isomorphism

$$\alpha : G/\ker(\varphi) \to \mathrm{im}(\varphi).$$

Using the notation from the previous section, where if $x \in G$ then $[x] \in G/\ker(\varphi)$ denotes the coset $x\ker(\varphi)$, let

$$\alpha([x]) = \varphi(x).$$

There are a number of things that we need to check. First, that α is well-defined.

Suppose $[x] = [x']$. Then $x\ker(\varphi) = x'\ker(\varphi)$, and so $x = xe = x'k$ for some $k \in \ker(\varphi)$. But then

$$\varphi(x) = \varphi(x'k) = \varphi(x')\varphi(k) = \varphi(x')e = \varphi(x'),$$

and so α is well-defined, as it doesn't make any difference which of the elements $x, x' \in [x]$ we use.

Next, let's prove that α is a homomorphism. This is true, since if $[x], [y] \in G/\ker(\varphi)$ then

$$\alpha([x][y]) = \alpha([xy]) = \varphi(xy) = \varphi(x)\varphi(y) = \alpha([x])\alpha([y]).$$

Now we just need to show that α is bijective. It is injective since

$$\begin{aligned} \alpha([x]) = \alpha([y]) &\Rightarrow \varphi(x) = \varphi(y) \\ &\Rightarrow \varphi(x^{-1}y) = e \\ &\Rightarrow y = x(x^{-1}y) \in x\ker(\varphi) \\ &\Rightarrow [x] = [y], \end{aligned}$$

since if two left cosets $[x] = x\ker(\varphi)$ and $[y] = y\ker(\varphi)$ have an element (y in this case) in common, then they are equal.

Finally, it is easy to see that α is surjective, since if $h \in \mathrm{im}(\varphi)$ then

$$h = \varphi(g) = \alpha([g])$$

for some $g \in G$. □

This means that finding a homomorphism between two groups immediately gives us lots of information about the kernel and image. To summarize:

Theorem 17.2. *Let* $\varphi : G \to H$ *be a homomorphism. Then* $\ker \varphi$ *is a normal subgroup of* G, $\mathrm{im}(\varphi)$ *is a subgroup of* H, *and* $\mathrm{im}(\varphi) \cong G/\ker(\varphi)$.

Example 17.1. Let S_n be the symmetric group of degree n, where $n > 1$. Let $\varphi : S_n \to (\mathbb{R} \setminus \{0\}, \times)$ be the homomorphism with $\varphi(\sigma) = 1$ if σ is an even permutation and $\varphi(\sigma) = -1$ if σ is an odd permutation. Then the kernel of φ is A_n and the image is $\{1, -1\}$, so $A_n \trianglelefteq S_n$ and

$$S_n/A_n \cong (\{1, -1\}, \times),$$

which is a cyclic group of order 2.

Example 17.2. Let D_{2n} be the dihedral group of order $2n$, and let $\varphi : D_{2n} \to (\mathbb{R} \setminus \{0\}, \times)$ be the homomorphism with $\varphi(x) = 1$ if x is a rotation and $\varphi(x) = -1$ if x is a reflection. Then the kernel of φ is the subgroup $\langle a \rangle < D_{2n}$, which is therefore a normal subgroup, and the image of φ is $\{1, -1\}$, so

$$D_{2n}/\langle a \rangle \cong (\{1, -1\}, \times).$$

Example 17.3. Let $\mathbb{R}_+$ denote the set of positive real numbers. Then $\mathbb{R}_+$ is a group under multiplication.

Let $\varphi : (\mathbb{R} \setminus \{0\}, \times) \to (\mathbb{R}_+, \times)$ be the map given by $\varphi(x) = |x|$ for $x \in \mathbb{R} \setminus \{0\}$. If $x, y \in \mathbb{R} \setminus \{0\}$, then $|xy| = |x||y|$, and so φ is a homomorphism. The kernel is $\{1, -1\}$ and the image is $\mathbb{R}_+$, so $\{1, -1\} \trianglelefteq \mathbb{R} \setminus \{0\}$ and

$$\mathbb{R} \setminus \{0\}/\{1, -1\} \cong \mathbb{R}_+.$$

Example 17.4. Let H be the cyclic subgroup of $G = \mathbb{Z} \times \mathbb{Z}$ generated by $(2, 3)$. Since G is abelian, every subgroup, and in particular H, is normal, so we can form the quotient group G/H. We'll show that $G/H \cong \mathbb{Z}$.

This will follow from the Homomorphism Theorem if we can find a surjective homomorphism $\varphi : G \to \mathbb{Z}$ with $\ker(\varphi) = H$.

Define $\varphi : G \to \mathbb{Z}$ by $\varphi(m, n) = 3m - 2n$. Then for $(m, n), (m', n') \in G$,

$$\begin{aligned} \varphi((m, n) + (m', n')) &= \varphi(m + m', n + n') \\ &= 3(m + m') - 2(n + n') \\ &= ((3m - 2n) + (3m' - 2n') \\ &= \varphi(m, n) + \varphi(m', n') \end{aligned}$$

so φ is a homomorphism (the group operation is addition for all the groups concerned).

It's easy to check that φ is surjective and that its kernel is H, so by the Homomorphism Theorem

$$G/H = G/\ker(\varphi) \cong \mathrm{im}(\varphi) = \mathbb{Z}.$$

We could replace $(2,3)$ with any element (a,b) where $\mathrm{hcf}(a,b) = 1$.

Example 17.5. We'll give a new proof that if $\mathrm{hcf}(m,n) = 1$ then

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

(This follows from what we proved earlier about direct products of cyclic groups.)

Define

$$\varphi : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

by $\varphi(a) = ([a]_m, [a]_n)$. Then for $a, b \in \mathbb{Z}$,

$$\varphi(a+b) = ([a+b]_m, [a+b]_n) = ([a]_m, [a]_n) + ([b]_m, [b]_n) = \varphi(a) + \varphi(b),$$

so φ is a homomorphism.

The kernel of φ is $mn\mathbb{Z}$, since

$$\begin{aligned} a \in \ker(\varphi) &\Leftrightarrow ([a]_m, [a]_n) = ([0]_m, [0]_n) \\ &\Leftrightarrow a \text{ is divisible by both } m \text{ and } n \\ &\Leftrightarrow a \text{ is divisible by } mn, \end{aligned}$$

since $\mathrm{hcf}(m,n) = 1$.

Again because of the fact that $\mathrm{hcf}(m,n) = 1$, φ is also surjective, and so the Homomorphism Theorem gives

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

18. GROUP ACTIONS

In this section we come full circle. We started by introducing the group of symmetries of an object as a way of understanding the object. But it turns out that one of the most powerful ways to understand a *group* is to find different objects that it "acts" as symmetries of in different ways. Here we'll just cover the basic ideas, but this is one of the main tools in more advanced group theory, such as you will see if you take the third year Group Theory unit.

The idea of a group action generalizes the idea that the symmetric group S_n "acts" on the set $\{1, \ldots, n\}$ by permuting the elements. More generally we can replace the symmetric group be any group, and the set $\{1, \ldots, n\}$ by any set, and we are led to the following definition.

Definition 18.1. A **group action** (or just **action**) of a group G on a set X is a function $G \times X \to X$, where we'll denote the image of (g, x) as $g \cdot x$, such that

(1) $e \cdot x = x$ for all $x \in X$, and
(2) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$.

Remark 18.1. The idea is that we think of the group element g as "acting" on the element $x \in X$, and sending it to another element $g \cdot x \in X$. Property (1) says that the identity $e \in G$ fixes every element of X, and property (2) says that "acting" on x by h and then by g is the same as acting by the single element gh, thus connecting the group structure of G with the way it can act on X.

Example 18.1. S_n acts on $\{1, \ldots, n\}$ by $\sigma \cdot x = \sigma(x)$.

Example 18.2. The dihedral group D_{2n} acts on the set of vertices of a regular n-sided polygon. For example, if we label the vertices anticlockwise $1, \ldots, n$ and, as usual, a is a rotation anticlockwise through an angle of $2\pi/n$ and b is a reflection in the line of symmetry through vertex 1, then

- $a \cdot 1 = 2$
- $a \cdot 2 = 3$
- $a \cdot n = 1$
- $b \cdot 1 = 1$
- $b \cdot 2 = n$
- $b \cdot n = 2$.

Example 18.3. The dihedral group D_8 acts on the set of two diagonals of a square. If we denote by C the diagonal joining vertices 1 and 3, and by D the diagonal joining vertices 2 and 4, then, for example,

- $a \cdot C = D$
- $a \cdot D = C$

- $b \cdot C = C$
- $b \cdot D = D$

This example and the previous one show that the same group can have natural actions on more than one set.

The next two examples show how actions arise naturally even for groups that are not necessarily defined as groups of symmetries.

Example 18.4. Let G be any group (with the group operation written multiplicatively), then G acts on itself (i.e., we're taking $X = G$) by

$$g \cdot x = gx \text{ for } g, x \in G.$$

Here the properties required for a group action follow from the definition of a group:

(1) $e \cdot x = ex = x$ by definition of the identity element, and
(2) $g \cdot (h \cdot x) = g(hx) = (gh)x = (gh) \cdot x$ by associativity.

Example 18.5. Let G be a group and $H \leq G$ a subgroup, and let X be the set of left cosets of H in G. Then

$$g \cdot (xH) = gxH$$

for $g, x \in G$ defines an action of G on X, since

(1) $e \cdot (xH) = exH = xH$ for and $xH \in X$, and
(2) $g \cdot (h \cdot (xH)) = g \cdot (hxH) = ghxH = (gh) \cdot (xH)$ for $g, h \in G$ and $xH \in X$.

Lemma 18.1. *If G acts on X, then, for each $g \in G$, the map $X \to X$ defined by $x \mapsto g \cdot x$ is bijective. In particlar, if $x, y \in X$ and $g \cdot x = g \cdot y$ for any $g \in G$ then $x = y$.*

Proof. For $x \in X$ and $g \in G$,

$$x = e \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x)$$

and

$$x = e \cdot x = (gg^{-1}) \cdot x = g \cdot (g^{-1} \cdot x),$$

so the function $x \mapsto g^{-1} \cdot x$ is inverse to the function $x \mapsto g \cdot x$. □

Remark 18.2. In fact, the map from G to $S(X)$ (the group of permutations of X) that sends g to the permutation $x \mapsto g \cdot x$ is a group homomorphism. We won't pursue this point of view here, but it is quite straightforward to prove.

There are natural and important subsets of G and X associated with an element of X when G acts on X.

Definition 18.2. Suppose G acts on X and $x \in X$. Then

(1) the **orbit** $G \cdot x$ of x is

$$\{g \cdot x : g \in G\} \subseteq X,$$

and

(2) the **stabilizer** G_x of x is

$$\{g \in G : g \cdot x = x\} \subseteq G.$$

Example 18.6. Let $G = S_n$ act on $X = \{1, \ldots, n\}$ in the usual way. Then $G \cdot x = X$ for every $x \in X$, since for every $y \in X$ there is a permutation σ with $\sigma(x) = y$. The stabilizer of $x = n$ is the group of permutations that fix n, and just permute $\{1, \ldots, n-1\}$.

Example 18.7. Let $G = D_8$ act on the set X of vertices of a square, labelled $1, \ldots, 4$ as usual. The orbit of every vertex is the whole of X, since for any two vertices, there is a symmetry (in fact, a rotation), taking one to the other. There are two symmetries that fix the vertex 1: the identity and the reflection b, so $G_1 = \{e, b\}$. There are also two symmetries fixing the vertex 2: the identity and the reflection in the diagonal joining vertices 2 and 4, which is a^2b, so $G_2 = \{e, a^2, b\}$.

Example 18.8. Taking the previous example, it's clear that any subgroup of D_8 also acts on the set of vertices of the square. Let $H = \langle b \rangle$ act. Then the orbit of 1 is just $\{1\}$ and the orbit of 3 is just $\{3\}$, since every element of H fixes 1 and 3. But b swaps vertices 2 and 4, so the orbits of 2 and 4 are both $\{2, 4\}$. H is the stabilizer of both 1 and 3, but the stabilizers of 1 and 3 are both the trivial group $\{e\}$.

Proposition 18.2. *Let G act on X, and let $x, y \in X$. Then*

$$G \cdot x \cap G \cdot y \neq \emptyset \Leftrightarrow G \cdot x = G \cdot y.$$

I.e., two orbits (for the same action) are either disjoint or equal.

Proof. Suppose $G \cdot x \cap G \cdot y \neq \emptyset$. Then we can choose $z \in G \cdot x \cap G \cdot y$, so that $z = g \cdot x = h \cdot y$ for some $g, h \in G$. Then

$$x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot z = g^{-1} \cdot (h \cdot y) = (g^{-1}h) \cdot y$$

and

$$y = h^{-1} \cdot (h \cdot y) = h^{-1} \cdot z = h^{-1} \cdot (g \cdot x) = (h^{-1}g) \cdot x.$$

If $k \in G$, then

$$k \cdot x = k \cdot \big((g^{-1}h) \cdot y\big) = (kg^{-1}h) \cdot y \in G \cdot y$$

and

$$k \cdot y = k \cdot \big((h^{-1}g) \cdot x\big) = (kh^{-1}g) \cdot x \in G \cdot x,$$

so $G \cdot x = G \cdot y$.

Conversely, if $G \cdot x = G \cdot y$ then $G \cdot x \cap G \cdot y$ contains $x = e \cdot x$, so is certainly not empty. □

Remark 18.3. This means that the set X is partitioned into the orbits, so that each element of X is in one and only one orbit. For example, for the action of $\langle b \rangle$ on the set of vertices of a square, we saw that the orbits are

$$\{1\}, \{2, 4\} \text{ and } \{3\}.$$

Theorem 18.3. *Let G act on X, and let $x \in X$. Then the stabilizer G_x is a subgroup of G.*

Proof. First, $e \cdot x = x$ by property (1) in the definition of a group action, so $e \in G_x$.

Suppose $g, h \in G_x$. Then by property (2) in the definition of a group action

$$\begin{aligned}(gh) \cdot X &= g \cdot (h \cdot x) \\ &= g \cdot x \text{ since } h \in G_x \\ &= x \text{ since } g \in G_x,\end{aligned}$$

and so $gh \in G_x$, so G_x is closed under multiplication.

Finally, if $g \in G_x$ then

$$\begin{aligned}g^{-1} \cdot x &= g^{-1} \cdot (g \cdot x) \text{ since } x \in G_x \\ &= (g^{-1}g) \cdot x \\ &= e \cdot x \\ &= x,\end{aligned}$$

and so $g^{-1} \in G_x$. So G_x is closed under taking inverses.

So $G_x \leq G$. □

One of the most useful basic results about group actions is the following theorem, that can be regarded as a generalization of Lagrange's Theorem (we'll explain how this works after proving the theorem).

Theorem 18.4 (Orbit-Stabilizer Theorem)**.** *Let G be a group acting on a set X, and let $x \in X$. Then*

$$|G : G_x| = |G \cdot x|,$$

so that, if G is finite.

$$|G| = |G \cdot x||G_x|.$$

Proof. Recall that the index $|G : G_x|$ is the number of left cosets of G_x in G, so we can prove the first equation by finding a bijection between the set of left cosets and the set $G \cdot x$.

Define $\alpha : G \to G \cdot x$ by $\alpha(g) = g \cdot x$. Then, for $g, h \in G$,

$$\begin{aligned}\alpha(g) = \alpha(h) &\Leftrightarrow g \cdot x = h \cdot x \\ &\Leftrightarrow (h^{-1}g) \cdot x = x \\ &\Leftrightarrow h^{-1}g \in G_x \\ &\Leftrightarrow gG_x = h(h^{-1}g)G_x = hG_x,\end{aligned}$$

so α induces a bijection $gG_x \mapsto g \cdot x$ between the set of left cosets and the set $G \cdot x$.

The second equation follows since, if G is finite, $|G| = |G : G_x||G_x|$. □

Example 18.9. Let $G = S_n$ act on $\{1, \ldots, n\}$ in the usual way. Then $G \cdot n = \{1, \ldots, n\}$, so $|G \cdot 1| = n$, and G_n is the group of permutations of $\{1, \ldots, n-1\}$, which has order $(n-1)!$.

So

$$|G| = n! = n\,((n-1)!) = |G \cdot n||G_n|.$$

Example 18.10. Let $H \leq G$ be finite groups and let G act on the set X of left cosets of H in G as described above. Then $H = eH$ is an element of X with stabilizer H (since $g \cdot H = gH$ is equal to H if and only if $g \in H$, and with orbit X with $|G : H|$ elements. So the Orbit-Stabilizer Theorem just says that

$$|G| = |G : H||H|,$$

which is just Lagrange's Theorem.

Example 18.11. Let $G = D_{2n}$ acting on the set of vertices of a regular n-sided polygon in the usual way, whhere b is the reflection in the line of symmetry through vertex 1. Then the orbit $G \cdot 1$ is the set of all n vertices, and the stabilizer G_1 is the subgroup $\{e, b\}$. So the Orbit-Stabilizer Theorem says

$$|G| = 2n = |G \cdot 1||G_1|.$$

Notice that if we didn't already know the order of D_{2n}, this would give a method of calculating it, which is actually very useful in more complicated examples.