M1J2 Group Theory 2018

Marie-Amelie Lawn

based on notes by Matthew Towers

Some good references for this course are:

- *A concise introduction to pure mathematics*, Martin Liebeck (510 LIE in the Central Library level 3). Mainly for the section on permutations.
- *A book of abstract algebra*, C.C. Pinter. Available as an ebook through the Imperial library website.

There are lots of introductory group theory textbooks: try a few and find one you like. *Visual group theory* by Nathan Carter is very different to standard textbooks and is worth looking at if you like to think geometrically.

Contents

Lecture 1

1 Basic definitions and examples

1.1 Binary operations and groups

Definition 1. *Let G be a set. A binary operation on G is a function*

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

Let (g, h) be an element of $G \times G$. We will denote the value of the function on the pair (g, h) by $g \star h$.

Recall that the Cartesian product $G \times G$ is defined as the set of ordered pairs (a, b) with a and b elements of G. Note that there are infinitely many binary operations possible on a set.

Example 1. *1) Let $\mathbb{Z}$ be the set of integers. The usual addition $+$ is a binary operation. Another possible binary operation on $\mathbb{Z}$ is the multiplication $\times$. But we can also define something less familiar like $g \star h := g^h$ for all g, h in $\mathbb{Z}$.*

*2) The usual substraction $-$ is **not** a binary operation on the set of strictly positive whole numbers $\mathbb{N}$, because it doesn't always output an element of $\mathbb{N}$.*

3) The usual substraction $-$ is a binary operation on the set of complex numbers $\mathbb{C}$.

4) There are many more arbitrary seeming examples. For example, let G be a set, then we could simply define $g \star h = h$ for all $g, h \in G$: to "combine" two elements, you always pick the second one. Another example is a "constant" binary operation: for a nonempty set G, choose once and for all an element $c \in G$, and define $g \star h = c$ for all $g, h \in G$.

Remark 1. *1) Note that since binary operations have inputs in the cartesian product $G \times G$, they are in general not commutative. In fact, for g, h two elements of G, the two ordered pairs (g, h) and (h, g) are not equal and hence in general $g \star h$ and $h \star g$ are not equal either.*

*2) If G is a finite set with n elements, i.e $G = g_1, \ldots, g_n$, then a binary operation on G can be described by a multiplication table or **Cayley table**:*

$\star$	g_1	g_2	$\cdots$	g_n
g_1	$g_1 \star g_1$	$g_1 \star g_2$	$\cdots$	$g_1 \star g_n$
$\vdots$				$\vdots$
g_n	$g_n \star g_1$	$g_n \star g_2$	$\cdots$	$g_n \star g_n$

Hence the number of different binary operations on G is n^{n^2}.

We will now consider some special binary operations with nice properties.

Definition 2. *A binary operation $\star$ on a set G is called associative if it satisfies*

$$g \star (h \star k) = (g \star h) \star k,$$

for all g, h, k in G.

Example 2. *1) The usual addition $+$ and the usual multiplication $\cdot$ on the sets $\mathbb{Z}, \mathbb{R}$ and $\mathbb{C}$ are associative.*

2) $-$ on $\mathbb{R}$ is not associative. In fact for example $2 - (3 - 4) \neq (2 - 3) - 4$.

3) $g \star h = g^h$ is not associative as $(2 \star 3) \star 2 = 2^3 \star 2 = 8^2 = 64$ and $2 \star (3 \star 2) = 512$.

Definition 3. *A binary operation $\star$ on a set G is called commutative if it satisfies*

$$g \star h = h \star g,$$

for all g, h in G.

Example 3. *1) The usual addition $+$ and the usual multiplication $\cdot$ on the sets $\mathbb{Z}, \mathbb{R}$ and $\mathbb{C}$ are commutative, the usual substraction $-$ is not as $5 - 7 = -2$, $7 - 5 = 2$.*

2) On $\mathbb{R}$, the operation defined by $g \star h := 1 + g \cdot h$ is commutative as the usual multiplication is, but it is not associative. In fact let $g = 0$, $h = 1$, $k = -1$, then

$$(g \star h) \star k = 1 \star -1 = 0, g \star (h \star k) = 0 \star 1 = 1.$$

Definition 4. *Let G be a set with a binary operation $\star$. An element e of G is called left (respectively right) identity (element) if for all g in G*

$$e \star g = g \text{ (respectively } g \star e = g).$$

Note that there might be many left (or right) identities, and that there might also be none.

Example 4. *1) Consider the operation $g \star h := g$ on a set G. By definition any h is a right identity. Assume now e is a right identity. Then $e \star h = h$, for all h in G. But $e \star h = e$ by definition of the operation. Hence $e = h$ and e has to be different for each h, therefore there is no left identity element.*

2) The operation $g \star h = 1 + g \cdot h$ hast no left or right identity element. In fact assume e is a right identity, then especially for $g = 1$, we have $1 = 1 \star e = 1 + 1 \cdot e$, hence $e = 0$. But now for $g = 2$, we should have $2 = 2 \star e = 2 \star 0 = 1 + 2 \cdot 0 = 1$, which is a contradiction.

This is annoying. We therefore want to know under which condition we can have "nicer" identity elements. This is given by the following propositions

Proposition 1. *Let G be a set with a binary operation $\star$ that has both a left identity e_1 and a right identity e_2. Then*

$$e_1 = e_2 =: e.$$

Proof. Let e_1 be the left identity, then for any element g in G, $e_1 \star g = g$. In particular if $g = e_2$, the right identity, we have $e_1 \star e_2 = e_2$. Similarly $e_1 \star e_2 = e_1$, as e_2 is the right identity, which proves the result. □

In this case e is called the (two-sided) identity element. Note that different operations on a set might have different identities. For examples $(\mathbb{R}, +)$ has identity 0, whereas $(\mathbb{R}, \cdot)$ has 1 as identity.

Proposition 2. *Let G be a set with an identity element e. Then e is unique.*

Proof. By definition $e \star g = g \star e = g$ for all g in G. Assume e' is another identity. Then $e' \star g = g \star e' = g$ for all g in G as well. In particular

$$e = e' \star e = e \star e' = e'.$$

□

The notion of identity leads us naturally to the notion of inverses.

Definition 5. *Let G be a set with a binary operation $\star$ and an identity element e. Let g be an element of G. An element h in G such that*

$$h \star g = e \text{ (resp. } g \star h = e)$$

is called left (resp. right) inverse of g.

Note that an element g in G can have no left or right inverse.

Example 5. *Consider the set of natural numbers $\mathbb{N}$ together with the usual multiplication $\cdot$. Except the number 1, no element has an inverse.*

The right inverse of an element is not necessarily equal to its left inverse and vice versa. We want to explore conditions under which they are actually equal.

Proposition 3. *Let G be a set with associative binary operation $\star$ and an identity element e. If h_1 is a left inverse and h_2 is a right inverse of an element g in G, then*

$$h_1 = h_2 =: g^{-1}.$$

Proof. Since h_1 is a left inverse we have by definition $h_1 \star g = e$, and since h_2 is a right inverse $g \star h_2 = e$. Hence, since the operation is associative

$$h_2 = e \star h_2 = (h_1 \star g) \star h_2 = h_1 \star (g \star h_2) = h_1 \star e = h_1,$$

which proves the result. □

In this case we call g^{-1} a (two-sided) inverse.

Proposition 4. *Let G be a set with associative binary operation and identity element e. If g is an element of G and g has an inverse, then g^{-1} is unique.*

Proof. Let $\tilde{g}^{-1}$ be another inverse of g. Then $\tilde{g}^{-1} \star g = g \star \tilde{g}^{-1} = e$. Moreover $g^{-1} \star g = g \star g^{-1} = e$. Hence since $\star$ is associative

$$g^{-1} = e \star g^{-1} = (\tilde{g}^{-1} \star g) \star g^{-1} = \tilde{g}^{-1} \star (g \star g^{-1}) = \tilde{g}^{-1} \star e = \tilde{g}^{-1}.$$

□

We are now ready to give the definition of a group, which is simply the data of a set together with a binary operation satisfying (some of) the nice properties we studied above. It is defined by a list of axioms as follows.

Definition 6. *A **group** $(G, \star)$ is a set G together with a binary operation $\star$ on G such that*

1) $\star$ is associative.

2) $\star$ has an identity element.

3) For all elements g in G, there exists an inverse g^{-1} in G.

The binary operation $\star$ is called the group operation.

Example 6. *1)* $(\mathbb{Z}, +)$ *is a group. In fact the usual addition is clearly associative,* 0 *is the identity and for each element* a *in* $\mathbb{Z}$ $-a$ *is an inverse.* $(\mathbb{R}, +)$ *and* $(\mathbb{C}, +)$ *are groups as well, but not* $(\mathbb{N}, +)$ *since for an element* a *in* $\mathbb{N}$, $-a$ *is not in* $\mathbb{N}$.

2) $(\mathbb{Z}, -)$ *is not a group since the usual substraction is not associative.*

3) $(\mathbb{C}, \cdot)$, *where* $\cdot$ *is the usual multiplication of complex numbers is not a group since the element* 0 *has no inverse. But* $(\mathbb{C}^*, \cdot)$ *is, and so is* $(\mathbb{R}^*, \cdot)$.

4) Let $G := \{e\}$, *a one element set, and let* $\star$ *be the binary operation on* G *defined by* $e \star e = e$. *Recall that there is only one binary operation on a one element set). Then* $(G, \star)$ *is a group, called the* ***trivial group****.*

Note that all examples above are sets of numbers but there are many other ways to get groups. Some examples are groups of special matrices, permutation groups, symmetry groups. We will study some of these examples later in the course.

Definition 7. *Let* $(G, \star)$ *be a group. If* G *is a finite set with exactly* n *different elements we write* $|G| = n$ *and say* G *has* ***order*** n, *and that* G *is a finite group. Otherwise we say that* $(G, *)$ *is an infinite group.*

Example 7. *Let* $G = \{1, -1, i, -i\}$ *a subset of* $\mathbb{C}$, *and* $\cdot$ *the usual multiplication of complex numbers. You can check as an exercise that* $(G, \cdot)$ *is a finite agroup.*

Definition 8. *Let* $(G, \star)$ *be a group. If* $\star$ *is commutative,* G *is called an Abelian group.*

All groups seen so far are Abelian since the usual addition and multiplication are commutative on $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$. But it is not always the case.

Example 8. *Let* G *be the set of invertible real functions and* $\mathbb{C}irc$ *the composition of functions.The identity on* G *is the identity function* $id : \mathbb{R} \to \mathbb{R}$, $x \mapsto x$. *All functions have an inverse by assumption, and the composition of function is associative, hence* $(G, \mathbb{C}irc)$ *is a group. But* $\mathbb{C}irc$ *is not commutative.*

1.2 Some consequences of the axioms of group

Let $(G, \star)$ be a group.

Remark 2. *By our previous considerations about binary operations and from the axioms of groups we deduce immediately that*

1) The identity element is unique by Proposition 2.

2) For all elements g *of* G, *the inverse* g^{-1} *is unique by Proposition 4.*

We have moreover the following

Proposition 5. *Let* $(G, \star)$ *be a group.,* g *an element of* G. *Then*

1) If either $g \star h = e$ *or* $h \star g = e$ *for some* h *in* G, *then* $h = g^{-1}$.

2) The inverse of g^{-1} *is* g *(i.e* $(g^{-1})^{-1} = g$*)*

Proof. 1) This follows immediately from Proposition 3 and from the existence of inverses for any element g In fact if $g \star h = e$, h is a right inverse (and a left inverse in the other case), hence $h = g^{-1}$.

2) $g \star g^{-1} = e$ by definition. The result follows immediately from part 1).

□

Lecture 2

Remark 3. *There are only two ways to bracket a product of three elements a, b, c of a group:*

$$a * (b * c) \quad or \quad (a * b) * c$$

and the associativity axiom tells you that these are equal, so that the product $a * b * c$ is unambiguous. But the associativity axiom doesn't tell you immediately that longer products are independent of how they are bracketed, for example, is

$$(a * b) * (c * d) \quad equal\ to \quad ((a * b) * c) * d?$$

In fact the answer is yes, for a product of any length: any bracketing you use to work out a product like $g_1 * \cdots * g_n$ gives the same result. You can prove this by induction: one such proof is given in the book by J.A. Green in the suggested reading.

Proposition 6. *Let $G, *$ be a group and $g, h \in G$. Then $(g * h)^{-1} = h^{-1} * g^{-1}$.*

Proof. We are going to show that $(h^{-1} * g^{-1}) * (g * h) = e$. We are free to bracket the product on the left in whichever way we like as discussed in the previous remark, so

$$(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * e * h = h^{-1} * h = e. \tag{1}$$

In a group, if $x * y = e$ then multiplying on the right by y^{-1} gives $x * y * y^{-1} = e * y^{-1}$ so $x = y^{-1}$. Applying that to (1) gives that $h^{-1} * g^{-1} = (g * h)^{-1}$ as required. □

There is some special notation for what happens when you multiply a group element by itself some number of times.

Definition 9. *Let $n \in \mathbb{Z}$, let $G, *$ be a group and let $g \in G$. Then we define g^n as follows:*

$$g^n = \begin{cases} g * g * \cdots * g & n > 0 \\ g^{-1} * g^{-1} * \cdots * g^{-1} & n < 0 \\ e & n = 0 \end{cases}$$

where in the first case there are n copies of g in the product and in the second there are $-n$ copies of g^{-1}, so that $g^n = (g^{-1})^{-n}$.

These exponents behave exactly how you would expect them to.

Proposition 7. *Let $n, m \in \mathbb{Z}$ and let $G, *$ be a group. Then*

1. $g^n * g^m = g^{n+m}$.
2. $(g^n)^m = g^{nm}$.

Proof. 1. This result is clear if either n or m is zero, and follows directly from associativity of $G, *$ if n and m have the same sign. So suppose $n > 0$ and $m < 0$. The proof is by induction on n, and when $n = 1$,

$$g * g^m = g * (\underbrace{g^{-1} * \cdots * g^{-1}}_{-m}) = (g * g^{-1}) * g^{m+1} = g^{m+1}$$

as required.

Now for $n > 1$ we have

$$g^n * g^m = g * g^{n-1} * g^m = g * g^{m+n-1}$$

by induction, and using either the base case (if $m + n - 1 < 0$) or the comment at the start of the proof, this equals g^{m+n} as required.

The case $n < 0$ and $m > 0$ is similar.

2. For m positive or zero this follows immediately from the definition, so suppose $m < 0$. We do the case $n > 0$. The first part of this proposition implies $(g^n)^{-1} = g^{-n}$, so

$$(g^n)^m = g^{-n} * \cdots * g^{-n}$$

with $-m$ copies of g^{-n} appearing. This is the product of $-mn$ copies of g^{-1}, so equals g^{mn} by definition.

The case when $n < 0$ is similar. □

Very often we'll write the product $g \star h$ of two group elements simply as gh, especially when the group operation $\star$ is some kind of multiplication.

1.3 Modular arithmetic and the group $\mathbb{Z}_n$

There are some nice examples of finite abelian groups that show up when we think about modular arithmetic. You should have met modular arithmetic before (in M1F), but let's recall the definitions.

Fix a positive integer n.

Definition 10. *For $a, b \in \mathbb{Z}$, we say that a is **congruent to** b **modulo** n (or just **mod** n) if $a - b$ is divisible by n. In this case we write*

$$a \equiv b \mod n.$$

For example $22 \equiv 4 \mod 9$, as $22 - 4 = 18$ and $9|18$.
We recall the following

Proposition 8. *Let a, b, c be in $\mathbb{Z}$. Then*

1) $a \equiv a \mod n$ (reflexivity).

2) If $a \equiv b \mod n$, then $b \equiv a \mod n$ (symmetry).

3) If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$ (transitivity).

The last proposition means exactly that congruences define an equivalence relation on $\mathbb{Z}$, and for any integer a we will write

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

for the equivalence class containing a, so $[a] = [a']$ if and only if the integers a and a' are congruent mod n. Every integer is congruent to exactly one of the numbers $0, 1, \ldots, n-1$, so there are exactly n equivalence classes. We write

$$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$$

for the set of equivalence classes.

We now want to define operations on this new set. In order to do this we recall the following

Lemma 1. *Suppose $a, a', b, b' \in \mathbb{Z}$ are integers such that $[a] = [a']$ and $[b] = [b']$. Then:*

1. $[a + b] = [a' + b']$.
2. $[ab] = [a'b']$.

Proof. This is an easy check that you should have seen in M1F. □

This lemma means that if we choose integers a and b and calculate $a + b$ or ab, and then you choose two other representatives $a' \in [a]$ and $b' \in [b]$ and calculate $a' + b'$ or $a'b'$ we get the same element of $\mathbb{Z}_n$. We can therefore define the following well-defined addition and multiplication on $\mathbb{Z}_n$:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [a + b]_n$$
$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [ab]_n.$$

Proposition 9. *$(\mathbb{Z}_n, +)$ is an Abelian group.*
Note that $(\mathbb{Z}_n, +)$ is a finite group, of size n.

Proof. The element $[0]_n$ is an identity element, any element $[a]_n$ has an inverse $[-a]_n$, and the operation is associative and commutative (because addition on $\mathbb{Z}$ is associative and commutative). □

Lecture 3

Now what about the set $(\mathbb{Z}, \cdot)$?

Example 9. *1) $(\mathbb{Z}_3, \cdot)$ is associative since the usual multiplication is associative and therefore*

$$([a] \cdot [b]) \cdot [c] = [ab] \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot ([b] \cdot [c]).$$

Similarly we can show that the operation is commutative. The identity is the element $[e]$ such that $[a] = [a] \cdot [e] = [e] \cdot [a] = [ae] = [ea]$, hence [e]=[1]. As for the inverses we find them looking at the Cayley table of $\mathbb{Z}_3$.

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	$4 \equiv 1 \mod 3$

Hence the inverse of $[1]$ *is* $[1]$*, the inverse of* $[2]$ *is* $[2]$*, but* $[0]$ *does not have an inverse, hence* $(\mathbb{Z}_3, \cdot)$ *is not a group.*
But $(\mathbb{Z}_3 - \{[0]\}, \cdot)$ *is an Abelian group.*

2) *For* $(\mathbb{Z}_4, \cdot)$ *the same consideration as above show that the operation is commutative and associative, and that* $[1]$ *is the identity. But similarly we can show that* $[0]$ *and* $[2]$ *do not have inverse elements, whereas* $[1]$ *and* $[3]$ *do (*$[1]^{-1} = [1]$ *and* $[3]^{-1} = [3]$*).*

Hence in general $(\mathbb{Z}_n, \cdot)$ is not a group. Nevertheless it is possible to correct this in the following way.

Lemma 2. *For each* $[a] \in \mathbb{Z}_n$*, there exists* $[b] \in \mathbb{Z}_n$ *such that* $[a][b] = [1]$ *if and only if* a *is coprime to* n*.*

We use the notation $(a, n) = 1$ for the greatest common divisor of a and n is 1, *i.e.* a is coprime to n.

Proof. Recall that $(a, n) = 1$ if and only if we can find integers b, c such that

$$ab + nc = 1$$

(this follows from Euclid's algorithm). Suppose that $(a, n) = 1$. Then we can find b, c such that $ab + nc = 1$, and then $ab \equiv 1 \mod n$ so $[a][b] = [1]$. Conversely, suppose there is a $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$. This means $ab \equiv 1 \mod n$, so $ab - 1 = nc$ for some integer c, and then $ab + nc = 1$. □

Definition 11.

$$\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n | \exists [b] \in \mathbb{Z}_n \text{ such that } [a][b] = [1]\}$$

of elements in $\mathbb{Z}_n$ *which have inverses.*

By Lemma 2 this is the set of $[a]$ such that $(a, n) = 1$.

Proposition 10. *The set* $(\mathbb{Z}_n^*, \cdot)$ *forms a finite Abelian group with the operation of multiplication.*

Proof. The only thing we really have to prove is that the set is closed under our multiplication. But if a and b are both coprime to n then ab is also coprime to n, so multiplication really does define a binary operation on $\mathbb{Z}_n^*$. The element $[1] \in \mathbb{Z}_n^*$ is an identity, and associativity and commutativity follow immediately from associativity and commutativity in $(\mathbb{Z}, \cdot)$. Finally if $[a] \in \mathbb{Z}_n^*$ then by definition there is a $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$, but then $[a]$ is the inverse to $[b]$ so $[b]$ must be in $\mathbb{Z}_n^*$. So $\mathbb{Z}_n^*$ has inverses. □

Notice that if n is a prime number then

$$\#\mathbb{Z}_n^* = n - 1$$

but if n is not prime then it's not immediately obvious how big $\mathbb{Z}_n^*$ is.

2 Cyclic groups

Definition 12. *Let G be a group, and let $g \in G$. The **order** of g is the smallest positive integer n such that*

$$g^n = e.$$

*If no such n exists we say that g has **infinite order**.*

Example 10. *In the group $(\mathbb{C}^*, \cdot)$ the element $-1 \in \mathbb{C}^*$ has order 2, and the element $i \in \mathbb{C}^*$ has order 4. The element $10 \in \mathbb{C}^*$ has infinite order.*

Remark 4. *Do not confuse the order of a group, i.e. the size of a (finite) group (*e.g. *"the group $\mathbb{Z}_5$ has order 5") with the order of an element.*

Lemma 3. *Let G be a finite group. Then every element of G has finite order.*

Proof. Let $g \in G$, and consider the elements

$$g, g^2, g^3, \ldots$$

of G. Since G is finite and this list is infinitely long, the elements of the list cannot all be different: we must have $g^a = g^b$ for some $a < b$. Then $g^{b-a} = e$, that is, some positive power of g equals the identity element. Thus the order of g is some number which is at most $b - a$. □

Lemma 4. *Suppose G is a group and $g \in G$ has order n. Then the elements $e = g^0, g, g^2, \ldots, g^{n-1}$ are all different.*

Proof. Suppose $g^i = g^j$ for some $0 \leq i < j \leq n - 1$. Then we can write $j = i + k$ for some $0 < k < n$. So $g^i = g^{i+k} = g^i g^k$. Multiplying both sides by $(g^i)^{-1} = g^{-i}$ we get $e = g^k$. But this contradicts n being the smallest positive power of g which equals the identity. □

Corollary 1. *If G is finite of size n, and $g \in G$, then the order of g is at most n.*

Definition 13. *A group G is called **cyclic** if there is a $g \in G$ such that*

$$G = \{g^n, n \in \mathbb{Z}\}.$$

*Any $g \in G$ with this property is called a **generator** of G.*

Example 11. *The group $(\mathbb{Z}, +)$ is cyclic, and the element $1 \in \mathbb{Z}$ is a generator (remember that in this group 'g^n' means the result of adding g to itself n times). There is exactly one other generator for this group namely -1.*

Example 12. *For any n, the group $(\mathbb{Z}_n, +)$ is cyclic and $[1]$ is a generator.*

Lemma 5. *Cyclic groups are abelian.*

Proof. Let G be a cyclic group and g be a generator. Take any two elements $h, k \in G$, then we have $h = g^i$ and $k = g^j$ for some $i, j \in \mathbb{Z}$. Hence

$$hk = g^i g^j = g^{i+j} = g^j g^i = kh.$$

□

The converse is false!

Example 13. *$(\mathbb{Q}, +)$ is abelian but is not cyclic. We can prove this by contradiction: if $q \in \mathbb{Q}$ was a generator, then we could write any rational number as nq for some integer n. But the number $q/2$ (for example) cannot be written in this form.*

Lemma 6. *Let G be a finite group of size n. Then G is cyclic if and only if G contains an element of order n.*

Proof. Suppose G is cyclic and $g \in G$ is a generator. Since G is finite, g must have finite order, d say. Then $G = \{e, g, g^2, ..., g^{d-1}\}$, and by Lemma 4 these elements are all distinct, so $d = n$.

Conversely suppose that G contains an element g of order n. Then the set $\{e, g, g^2, ..., g^{n-1}\}$ has size n so it is the whole of G. □

Example 14. *In the group $(\{1, -1, i, -i\}, \times)$ the elements i and $-i$ both have order 4, so this group is cyclic, and either of these elements is a generator.*

Lecture 4

Lemma 7. *Let G be a finite group then if G is cyclic, it has at most one element of order 2.*

Proof. Since G is finite, say of size n, there exists an element g in G of order n. Hence $g^n = e$. Any other element is of the form g^i, with $0 < i \leq n - 1$ as G is cyclic. Assume now that g^i is of order 2. Then

$$e = (g^i)^2 = g^{2i}, \text{ hence } 2i = n,$$

and $i = \frac{n}{2}$, which is only possible for one element in the case where n is even. If n is odd there is no element of order 2. □

Example 15. *$G = (\mathbb{Z}_5, \cdot)$ is not cyclic. In fact G has 8 elements (the number of classes of numbers which are coprime to 15), i.e.*

$$\mathbb{Z}_{15} = \{[1], [2], [4], [7], [8], [11], [13], [14]\}.$$

Hence it is a finite group of size 8. But $[4]^2 = [1]$ and $[14]^2 = [-1]^2 = [1]$, hence it has two elements of order 2. By our previous lemma it cannot be cyclic.

3 The symmetric groups

This family of examples is important enough to deserve its own section. See also Chapter 20 of Liebeck *A concise introduction to pure mathematics.*

3.1 Permutations

Recall the following definition from M1F

Definition 14. *A function f from a set X to a set Y is called*

- ***one-to-one** or **injective** if $f(x_1) = f(x_2)$ implies $x_1 = x_2$ for any $x_1, x_2 \in X$.*
- ***onto** or **surjective** if for every $y \in Y$ there is an $x \in X$ such that $f(x) = y$.*

- *a **bijection** if it is both injective and surjective.*

Furthermore, f is a bijection if and only if there is an inverse function $g : Y \to X$ such that $g \circ f$ is the identity function on X and $f \circ g$ is the identity function on Y.

Definition 15. *A **permutation** (on n symbols) is a bijection*

$$\sigma : \{1, ..., n\} \widetilde{\to} \{1, ..., n\}.$$

If we want to write down a permutation, one option is to use *two-row notation*. We write down the numbers 1 to n, and underneath each number i we write down the number that σ sends i to:

$$\begin{vmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{vmatrix}.$$

Because σ is a bijection, the bottom row of the table consists of the numbers $1, 2, \dots, n$ in some order. So a permutation is a 're-ordering' of the numbers 1 to n.

Example 16. *Let σ and τ be the functions:*

$$\begin{aligned} \sigma : \{1,2,3\} &\to \{1,2,3\} \\ 1 &\mapsto 1 \\ 2 &\mapsto 3 \\ 3 &\mapsto 2 \end{aligned} \qquad \begin{aligned} \text{and } \tau : \{1,2,3\} &\to \{1,2,3\} \\ 1 &\mapsto 2 \\ 2 &\mapsto 3 \\ 3 &\mapsto 1 \end{aligned}$$

These are both bijections, so they are permutations (on 3 symbols). In two-row notation we would write them as

$$\sigma = \begin{vmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{vmatrix} \text{and} \tau = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{vmatrix}.$$

Definition 16. *The set*

$$S_n = \left\{\sigma : \{1, ..., n\} \widetilde{\to} \{1, ..., n\}\right\}$$

*of all permutations on n symbols is called the **symmetric group** (on n symbols).*

Notice that S_n is not a set of numbers but a set of functions.

We are going now to justify why we called S_n the symmetric *group*. Define the binary operation on S_n as the composition of functions

$$(\sigma, \tau) \mapsto \sigma \circ \tau.$$

This makes sense because if σ and τ are bijections from $\{1, ..., n\}$ to $\{1, ..., n\}$ then their composition

$$\sigma \circ \tau : \{1, ..., n\} \to \{1, ..., n\}$$

is also a bijection. We are now ready to prove the following

Proposition 11. *$(S_n, \circ)$ is a group.*

Proof. The composition of functions is associative. The identity function Id on the set $\{1, ..., n\}$ is an element of S_n, and it satisfies $Id \circ \sigma = \sigma \circ Id = \sigma$ for any permutation $\sigma \in S_n$, so it is an identity element. Any $\sigma \in S_n$ is a bijection, so it has an inverse bijection $\sigma^{-1} \in S_n$ which satisfies $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = Id$. □

Example 17. *In Example 16 we wrote down two elements σ and τ of the group S_3. Let us compute their products, $\sigma \circ \tau$ and $\tau \circ \sigma$.*

Two-row notation is quite convenient for this. Take the table for τ, and look at its bottom row: in the ith column, we have the number $\tau(i)$. Now create a third row, where underneath each number $\tau(i)$ we write the number $\sigma(\tau(i))$ that we get by applying σ (this can be read off from the table for σ). In this case we get:

$$\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 2 & 1 \end{vmatrix}$$

and we can conclude that

$$\sigma \circ \tau = \begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{vmatrix}.$$

In a similar way we can compute that $\tau \circ \sigma = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{vmatrix}$. Note that $\sigma \circ \tau$ is in general not equal to $\tau \circ \sigma$. Hence $(S_n, \cdot$ is not an Abelian group.

Proposition 12. *$\#S_n = n!$.*

Proof. Define an element $\sigma \in S_n$ by specifying the outputs

$$\sigma(1), \sigma(2), ..., \sigma(n)$$

one-by-one. There are n possibilities for $\sigma(1)$. Then the number $\sigma(2)$ cannot be equal to $\sigma(1)$ (because σ has to be a bijection) so there are $n-1$ possibilities for $\sigma(2)$. Similarly $\sigma(3)$ cannot equal $\sigma(1)$ or $\sigma(2)$, so there are there are $n-2$ possibilities for it. Altogether this gives

$$n \times (n-1) \times \cdots \times 2 \times 1 = n!$$

elements of S_n. □

3.2 Cycle notation

There is a another way to write down elements of S_n, called *cycle notation.*

Definition 17. *A permutation $\sigma \in S_n$ is called a **cycle** if there is a sequence of distinct numbers $a_1, ..., a_k \in \{1, ..., n\}$ such that*

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

and $\sigma(i) = i$ for every number not in this sequence.

The number k is called the *length* of the cycle, and we often abbreviate 'cycle of length k' to 'k-cycle'.

Example 18. *Look at the following two permutations in S_4:*

$$\sigma = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{vmatrix} \text{ and } \tau = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{vmatrix}.$$

The first one is a 3-cycle, it rotates the numbers 1, 2, 3 and fixes 4. The second one is not a cycle: no numbers are fixed, so if it was a cycle it would have to be a 4-cycle, but it is not.

Note that a k-cycle is just a particular element of the group $(S_n \cdot)$, and therefore it makes sense to speak of its order.

Proposition 13. *The order of a k-cycle is k.*

Proof. By definition $\sigma^k = Id$, hence the order of σ is at most k. We need to prove that it is not less than k. Assume the order is $d < k$. Then we get immediately from the definition of cycle that $\sigma^d(a_1) = a_d \neq a_1$, hence $\sigma^d \neq Id$. □

In cycle notation, we write

$$(a_1, a_2, ..., a_k)$$

to mean the cycle which sends $a_1 \mapsto a_2 \mapsto ... \mapsto a_k \mapsto a_1$ and fixes all other elements. This only makes sense if the numbers $a_1, ..., a_k$ are all distinct (or this permutation would not be a cycle).

Example 19. *In cycle notation, we would write the 3-cycle σ from Example 18 as $(1, 2, 3)$.*

Remark 5.

1. *The cycle notation is ambiguous and you need to precise which S_n you are in.*
2. *There are several different ways to write the same cycle, for example $(1, 2, 3)$, $(2, 3, 1)$ and $(3, 1, 2)$ are all the same permutation. The usual convention is to put the smallest number first.*
3. *A cycle of length one has to be the identity permutation. So the 1-cycles (1), or (3), or (9), all denote the identity. The usual convention is to use (1), and this makes sense in any S_n.*
4. *Cycles only make sense if all elements are distinct.*

Example 20. *The permutation $\tau \in S_4$ from Example 18 is not a cycle, but it's easy to see that it can be expressed as the composition*

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

of two 2-cycles.

Definition 18. *We say that two cycles $(a_1, ..., a_k)$ and $(b_1, ..., b_m)$ are **disjoint** if no a_i is equal to any b_j.*

Disjoint cycles commute if these two cycles are disjoint (exercise).*i.e.*

$$(a_1, ..., a_k)(b_1, ..., b_m) = (b_1, ..., b_m)(a_1, ..., a_k).$$

Lemma 8. *Let $\sigma \in S^n$ be a permutation.*

1. *For any $i \in \{1, ..., n\}$, there is a positive integer d such that $\sigma^d(i) = i$.*
2. *If d is the smallest positive integer such that $\sigma^d(i) = i$, then the numbers $i, \sigma(i), \sigma^2(i), ..., \sigma^{d-1}(i)$ are all distinct.*
3. *If $j \in \{1, ..., n\}$ is not in the set $\{i, \sigma(i), ..., \sigma^{d-1}(i)\}$, then neither is $\sigma(j)$.*

Proof. 1. Since S^n is finite (recall that it has $n!$ elements), all elements have finite order, therefore $\sigma^d = Id$ for positive integer d, so certainly $\sigma^d(i) = i$.

2. Suppose $\sigma^k(i) = \sigma^l(i)$ for two integers $0 \leq k < l < d$. Then $\sigma^{l-k}(i) = i$, contradicting the fact that $d > l - l$ is the smallest integer with this property.

3. If $\sigma(j) = \sigma^k(i)$ for some k then $j = \sigma^{k-1}(i)$ and j is in the set whenever $\sigma(j)$ is which is a contradiction.

□

Proposition 14. *Any permutation can be expressed as a product of some number of disjoint cycles.*

Proof of Proposition 14. The proof is given by an explicit algorithm. Pick any $\sigma \in S_n$.

Step 1: Pick any number $i \in \{1, ..., n\}$. By Lemma 8(1)) there exists an integer d such that $\sigma^d(i) = i$. Take the smallest such d. Since by Lemma 8(2)) the elements $i, \sigma(i), \sigma^2(i), ..., \sigma^{d-1}(i)$ are all distinct, we cand form the cycle

$$\big(i, \sigma(i), ..., \sigma^{d-1}(i)\big)$$

Step 2: Pick any $j \in \{1, ..., n\}$ which does not occur in this cycle, and apply Step 1 to j to form another cycle. By Lemma 8(3), this new cycle is disjoint from the previous one.

Step 3: Pick any $k \in \{1, ..., n\}$ not occuring in any of our previous cycles. Applying Step 1 produces a new cycle, disjoint from each of our previous ones. Repeat this step until all numbers in $\{1, ..., n\}$ occur in one of our cycles.

The permutation σ will be the product of our list of cycles. □

The choices we make in this algorithm don't affect which cycles appear in our list, only the order in which they appear (and since disjoint cycles commute this is not important). Once we've factored σ into disjoint cycles $\gamma_1\gamma_2...\gamma_r$ we can record the lengths $(k_1, k_2, ..., k_r)$ of the cycles that occur; this list is called the **cycle-type** of σ.

Example 21. *Let's run this algorithm on the permutation*

$$\sigma = \begin{vmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 3 & 2 & 6 & 7 & 5 \end{vmatrix}.$$

At the first step we choose the number 1. *We have* $\sigma(1) = 4, \sigma^2(1) = \sigma(\sigma(1)) = 2, \sigma^3(1) = \sigma(2) = 1$. *So the first cycle is* $(1, 4, 2)$.

Not all of the numbers $1, 2, \ldots, 7$ *appear in this cycle, so we go back to step one and pick one that doesn't appear, say* 3. *Since* $\sigma(3) = 3$, *the cycle that we add is just* (3), *so we now have* $(1, 4, 2)(3)$.

We still haven't covered all the numbers, so pick a number that hasn't appeared yet, say 5. We have $\sigma(5) = 6, \sigma^2(5) = \sigma(6) = 7, \sigma^3(5) = \sigma(7) = 5$, *and so the cycle we add is* $(5, 6, 7)$ *and we now have*

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

Since all seven numbers now appear, the algorithm stops. The permutation σ *is the product of these three cycles, but the 1-cycle* (3) *is the identity permuation, so we can just write*

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

The cycle-type of σ *is* $(3, 3)$ *(we can leave out the 1's from this list, they're not important).*

4 Subgroups

4.1 Basic definitions

We have seen before that a group can be a subset of another group, for example $(\mathbb{R}, +)$ lives inside of $(\mathbb{C}, +)$. This consideration yields the concept of a subgroup.
In the following for more convenience we will write gh instead of the product $g \star h$ for two elements of a group.

Definition 19. *Let $(G, \star)$ be a group and let $H \subseteq G$ be a subset. We say that H is a **subgroup** of G if:*

1. *For any $g, h \in H$ we have $gh \in H$.*
2. *The identity element $e \in G$ lies in H.*
3. *If $g \in H$ then $g^{-1} \in H$.*

We denote a subgroup H of G by $H \leq G$.

Note that the first property guarantees that $\star$ defines a binary operation on H, and then the other two axioms guarantee that $(H, \star)$ is a group (associativity holds in G, and therefore automatically in H). So we can always think of a subgroup as being a group in its own right.

The second property guarantees that the subgroup H is non-empty. Conversely if we assume that G is non-empty we can remove the second property, since then there exists an element g in H, and its inverse g^{-1} is in H as well by property 3. But by the closure of H under multiplication $gg^{-1} = e$ is in H.

Example 22. *1) Let $G = \{1, -1, i, -1\} \subset \mathbb{C}^*$ and let $H \subset G$ be the subset $H = \{1, -1\}$. Then G is a subgroup of $(\mathbb{C}^*, \cdot)$, and H is a subgroup of G. But the subset $\{1, i\}$ does not form a subgroup as $i \cdot i = -1$, which is not an element of the subset.*

2) Let n be a fixed integer and $n\mathbb{Z} := \{nz | z \in \mathbb{Z}\}$. Then $(n\mathbb{Z}, +)$ is a subgrou of $(\mathbb{Z}, +)$.

3) Not every subset of a group which is closed under the binary operation is necessarily a subgroup. For example $(\mathbb{N}, +) \subset (\mathbb{Z})$ is closed under the addition but has no inverses.

4) Let $J := \{2n + 1 | n \in \mathbb{Z}\}$, the set of odd integers. $(J, +)$ is not a subgroup as the sum of two odd numbers is even.

5) $(\mathbb{Q}^*, \cdot)$ is a subgroup of $(\mathbb{R}^*, \cdot)$, which is itself a subgroup of $(\mathbb{C}^*, \cdot)$.

6) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

Example 23. *Any group G has two obvious subgroups: The subset with only element the identity $\{e\} \subseteq G$ and the group itself $G \subseteq G$.*

Definition 20. *Let G be a group. The subgroup $\{e\} \subseteq G$ is called the **trivial** subgroup.*
*A subgroup is called **proper** if it is not equal to G, and **non-trivial** if it is not equal to the trivial subgroup.*

Proposition 15. *(Subgroup test) Let $(G, \star)$ be a group and H be a non-empty subset of G such that if x, y are elements of H, then $x \star y^{-1}$ is in H.*
Then H is a subgroup of G.

Proof. We prove that H is indeed a group.
H contains the identity e: we know that if x, y are elements of H, then $x \star y^{-1}$ is in H. Let $x = y$. Then $e = x \star x^{-1} \in H$.
H contains inverses: Let x be an element of H. We saw that e is in H, hence $x^{-1} = e \star x^{-1}$ is in H.
H is closed under the binary operation: Let x and y be in H, then y^{-1} is H as we saw, and therefore $x \star y^{-1^{-1}}$ is in H. □

Example 24. *We says that a permutation $\sigma \in S_n$ such that $\sigma(i) = i$ fixes the element i. Let H be the subset of S_n consisting of all permutations fixing 1. We'll show that H is a subgroup using the subgroup test.*

Firstly, H is non-empty, since it certainly contains the identity permutation which fixes everything. Secondly, suppose $\sigma_1, \sigma_2 \in S_n$ fix 1. Then $\sigma_1(1) = 1$, so $\sigma_1^{-1}(1) = 1$. Therefore $(\sigma_1^{-1} \circ \sigma_2)(1) = \sigma_1^{-1}(\sigma_2(1)) = \sigma_1^{-1}(1) = 1$. It follows $\sigma_1^{-1} \circ \sigma_2 \in H$, and so H is a subgroup of S_n by the subgroup test.

4.2 Cyclic subgroups

Definition 21. *Let $(G, *)$ be a group, let $g \in G$, and let $\langle g \rangle = \{g^i : i \in \mathbb{Z}\}$. Then $\langle g \rangle$ is called the **cyclic subgroup generated by** g.*

The following lemma tells us that this set is indeed a group.

Lemma 9. *$\langle g \rangle \leq G$.*

Proof. Apply the subgroup test: $\langle g \rangle$ contains g so it is not empty, and if g^i, g^j are elements of $\langle g \rangle$ then $g^i \star (g^j)^{-1} = g^i * g^{-j} = g^{i-j} \in \langle g \rangle$. So the subgroup test implies $\langle g \rangle \leq G$. □

Lemma 10. *If g has order n, then $\langle g \rangle$ has order n.*

Proof. We know from Lemma 4 that the elements $e, g, g^2, \ldots, g^{n-1}$ of $\langle g \rangle$ are all different, so the size of $\langle g \rangle$ is at least n. We'll show that it is exactly n by showing that any $g^i \in \langle g \rangle$ equals one of these elements.

We can write $i = qn + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < n$ by the division algorithm. So

$$g^i = g^{qn+r} = g^{qn} * g^r = (g^n)^q * g^r = e^q * g^r = e * g^r = g^r.$$

Thus any element of $\langle g \rangle$ equals one of $e, g, \ldots, g^{n-1}$, and we're done. □

Example 25. *Consider $\langle (1,2) \rangle \leq S_3$. The permutation $(1,2)$ has order two, so $\langle (1,2) \rangle$ has size two, and its elements are $\{e, (1,2)\}$.*

Note that obviously if the group is not of finite size, then an element g in the group does not necessarily have finite order, and therefore $\langle g \rangle$ does not necessarily have finite size:

Example 26. *Consider the group $(\mathbb{Z}, +)$, n an integer. Then $\langle n \rangle = n\mathbb{Z}$.*

Example 27. *The order of $[2] \in \mathbb{Z}_6$ is 3, because $[2]^2 = [2] + [2] = [4]$ and $[2]^3 = [2] + [4] = [6] = [0]$, which is the identity element of $(\mathbb{Z}_6, +)$. Thus the cyclic subgroup generated by $[2]$ is $\langle [2] \rangle = \{[0], [2], [4]\} \leq \mathbb{Z}_6$.*

5 Cosets and Lagrange's Theorem

Definition 22. *Let $(G, *)$ be a group, H a subgroup of G, and g an element of G.*

1) The left coset of H by g is $gH := \{g \star h : h \in H\}$.

2) The right coset of H by g is $Hg := \{h \star g : h \in H\}$.

We write $G : H$ for the set of left cosets of H by elements of G so $G : H = \{gH : g \in G\}$. Similarly $H : G$ is the set of right cosets of H by elements of G.

Usually right cosets are not equal to left cosets for a particular subgroup H. Note that this is true if G is Abelian, but the converse is not true (this fact yields the study of normal subgroups).

Example 28. *The 3-cycle $(1,2,3) \in S_4$ has order 3, so $H := \langle (1,2,3) \rangle$ is equal to*

$$\{e, (1,2,3), (1,2,3)^2\} = (1,3,2).$$

Then

$$\begin{aligned} (1,2)H &= \{(1,2), (1,2)(1,2,3), (1,2)(1,3,2)\} \\ &= \{(1,2), (2,3), (1,3)\} \\ H(1,2) &= \{(1,2), (1,2,3)(1,2), (1,3,2)(1,2)\} \\ &= \{(1,2), (1,3), (2,3)\}. \end{aligned}$$

So in this case, $(1,2)H = H(1,2)$.

Example 29. *The 2-cycle $(1,2) \in S_3$ has order 2, so $H := \langle (1,2) \rangle$ is equal to $\{e, (1,2)\}$. Then*

$$\begin{aligned} (2,3)H &= \{(2,3), (2,3)(1,2)\} = \{(2,3), (1,3,2)\} \\ H(2,3) &= \{(2,3), (1,2)(2,3)\} = \{(2,3), (1,2,3)\} \end{aligned}$$

So in this case $(2,3)H \neq H(2,3)$.

Example 30. *Consider the group $(\mathbb{Z}, +)$. The subset of even integers $H = 2\mathbb{Z} \subset \mathbb{Z}$ is, as we saw, a subgroup. The subset $J = \{2z + 1 | z \in \mathbb{Z}\} \subset \mathbb{Z}$ of odd integers is not a subgroup, but it is closely related to the subgroup H. For instance, we can describe J as the set*

$$J = \{1 + n,\ n \in H\}.$$

In fact, if a is any odd integer then we have

$$J = \{a + n,\ n \in H\}.$$

Obviously J is the coset of H by a. Notice that we get the same coset when we start from any odd integer, and then add on all possible even integers. A concise notation for this is to write

$$J = a + H$$

(for some odd integer a). Also notice that every integer lies in either H or J, but not both.

Example 31. *Consider again the group $(\mathbb{Z}, +)$, but now consider the subgroup $H = 3\mathbb{Z} \subset \mathbb{Z}$ of all multiples of 3. The coset*

$$1 + H = \{1 + n,\ n \in 3\mathbb{Z}\}$$

*is exactly the set of numbers that are equal to 1 modulo 3 (*i.e. *it is the class $[1]$ in $\mathbb{Z}_3$). Again the number 1 can be replaced by any integer a such that $a \equiv 1 \mod 3$ then*

$$a + H = \{a + n,\ n \in 3\mathbb{Z}\} = 1 + 3\mathbb{Z}$$

so these two cosets are the same. Similarly, if b is any integer such that $b \equiv 2 \mod 3$ then the coset

$$b + H = \{b + n,\ n \in 3\mathbb{Z}\} = 2 + 3\mathbb{Z}$$

is the set of integers that equal 2 modulo 3. There is a third case; if c is an integer such that $c \equiv 0 \mod 3$ then

$$c + H = 3\mathbb{Z}$$

is the set of integers that are zero modulo 3. Notice that every integer lies in exactly one of these three cosets. Note that the coset $a + H$ does not depend on the element a as long as a is in the coset.

Proposition 16. *Let $(G, \star)$ be a group, and H as subgroup of G. For two elements g_1 and g_2, the cosets g_1H and g_2H are the same if and only if g_2 is an element of g_1H.*

Proof. Assume that $g_1H = g_2H$. Then since e is in H, $g_2 = g_2e$ is in g_2H, hence g_2 is in g_1H as well.
Conversely, suppose $g_2 \in g_1H$, which by definition means there is some $h \in H$ such that $g_2 = g_1h$. We will show firstly that $g_2H \subset g_1H$, and secondly that $g_1H \subset g_2H$, hence the two subsets are identical.

Any element in g_2H is of the form g_2k for some $k \in H$, and then

$$g_2k = (g_1h)k = g_1(hk).$$

The product hk lies in H (because H is a subgroup), so $g_1(hk)$ is an element of g_1H. This proves that $g_2H \subset g_1H$.

Now take an element in g_1H, it must be of the form g_1l for some $l \in H$. Then

$$g_1l = (g_2h^{-1})l = g_2(h^{-1}l).$$

The element $h^{-1}l$ lies in H (because H is a subgroup) so this is an element of g_2H. This proves that $g_1H \subset g_2H$. □

Corollary 2. *Every element $g \in G$ lies in exactly one of the left cosets of H.*

Proof. We know that $g \in gH$. If $g \in g'H$ for some g' then the previous proposition tells us that the coset $g'H$ is exactly the same subset as gH. □

The left cosets form a **partition** of G, they are a collection of subsets $g_1H, g_2H, ... \subset G$ such that

$$G = \bigcup g_iH$$

and the intersection of any two of these subsets is empty.

Example 32. *Consider the group $(\mathbb{Z}_6, +)$, and the cyclic subgroup*

$$H = \langle [3] \rangle = \{[0], [3]\}.$$

The cosets of H are

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

(this group is abelian so there is no distinction between left and right cosets). Notice that all three cosets have the same size.

Lemma 11. *Let G be a group and let $H \subset G$ be a finite subgroup. Then all left cosets of H have the same size,* i.e.

$$\#gH = \#H$$

for any $g \in G$.

Proof. Fix any $g \in G$. Now define a function

$$\alpha : H \to gH \tag{2}$$
$$h \mapsto gh. \tag{3}$$

This function is an injection, because if $\alpha(h_1) = \alpha(h_2)$ then $gh_1 = gh_2$, and multiplying on the left by g^{-1} shows that $h_1 = h_2$. It is also a surjection, because any element in gH is of the form $gh = \alpha(h)$ for some $h \in H$.

So α is a bijection, and hence the sets gH and H must have the same size. □

Remark 6. *If H is infinite (like in our earlier Examples 30 and 31) then the function α is still a bijection from H to gH, but the question of whether H and gH have 'the same size' is a bit more delicate.*

Theorem 1. *(Lagrange Theorem) Let G be a finite group and H be a subgroup, then*

$$\#G = \#H \cdot \#(G : H),$$

in particular the order of H divides the order of G.

Proof. We saw that the cosets of H form a partition of G, i.e. $G = \bigcup g_i H$. But $\#gH = \#H$, hence each piece of the partition has size the size of H, hence the size of G is the number of cosets times the size of H. □

Example 33. *The group $(\mathbb{Z}_{10}, +)$ has size 10, hence it has no subgroup of size $3, 4, 6, 7, 8$ or 9.*

Corollary 3. *Let G be a finite group and let $g \in G$. Then the order of g divides the size of G.*

Proof. The order of g equals the size of the cyclic subgroup $\langle g \rangle \subset G$. By Lagrange's theorem this divides $\#G$. □

In particular, if $g \in G$ is any element of a finite group, we must have

$$g^{\#G} = e.$$

Corollary 4. *Let G be a finite group of size p, where p is a prime number. Then G is cyclic.*

Proof. Pick any $g \in G$ not equal to e. Consider the cyclic subgroup $\langle g \rangle \subset G$. Its size divides p by Lagrange's theorem, so it is 1 or p (since p is prime). It cannot be 1 since $\langle g \rangle$ contains both g and e, so it must be p and therefore

$$\langle g \rangle = G.$$

So G is cyclic and g is a generator. □

Corollary 5 (Fermat's Little Theorem)**.** *Let $a \in \mathbb{Z}$ and let p be a prime number. If $a \not\equiv 0 \mod p$ then*

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

Proof. The group $(\mathbb{Z}_p^*, \times)$ has size $p-1$, so the element $[a] \in \mathbb{Z}_p^*$ satisfies

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

□

Another way to say this is that

$$a^p \equiv a \mod p$$

and this is still true if p does divide a.