Chapter 3

Introducing Groups

> *"We need a super-mathematics in which the operations are as unknown as the quantities they operate on, and a super-mathematician who does not know what he is doing when he performs these operations. Such a super-mathematics is the Theory of Groups." (Sir Arthur Stanley Eddington, physicist)*

The first two chapters dealt with planar geometry. We identified what are the possible planar isometries, and then, given a set S of points in the plane, we focused on the subset of planar isometries that preserves this given set S. These are called symmetries of S. We saw that planar isometries, respectively symmetries, can be composed to yield another planar isometry, respectively symmetry. Every planar isometry is invertible. Every symmetry of a given set S is invertible as well, with as inverse another symmetry of S.

We now put a first step into the world of abstract algebra, and introduce the notion of a *group*. We will see soon that groups have close connections with symmetries!

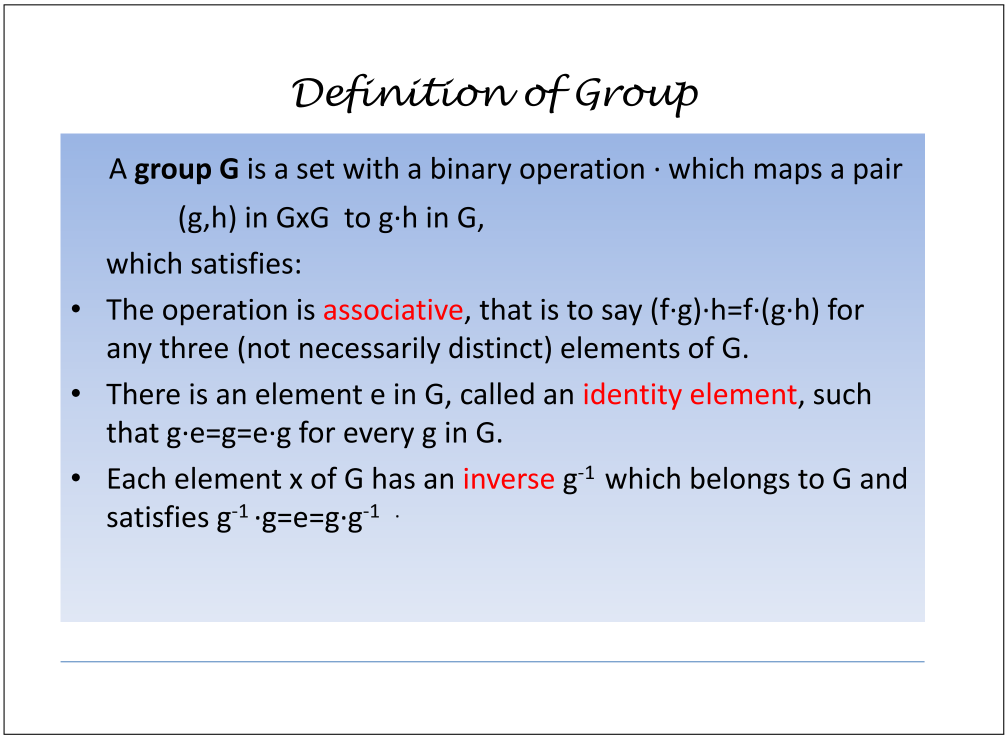
Definition 4. A group G is a set with a binary operation (law) $\cdot$ satisfying the following conditions:

1. For all $g_1, g_2 \in G \Rightarrow g_1 \cdot g_2 \in G$.

2. The binary law is associative.

3. There is an *identity* element e in G, such that $g \cdot e = e \cdot g = g$, $\forall g \in G$.

4. Every element $g \in G$ has an *inverse* g^{-1}, such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

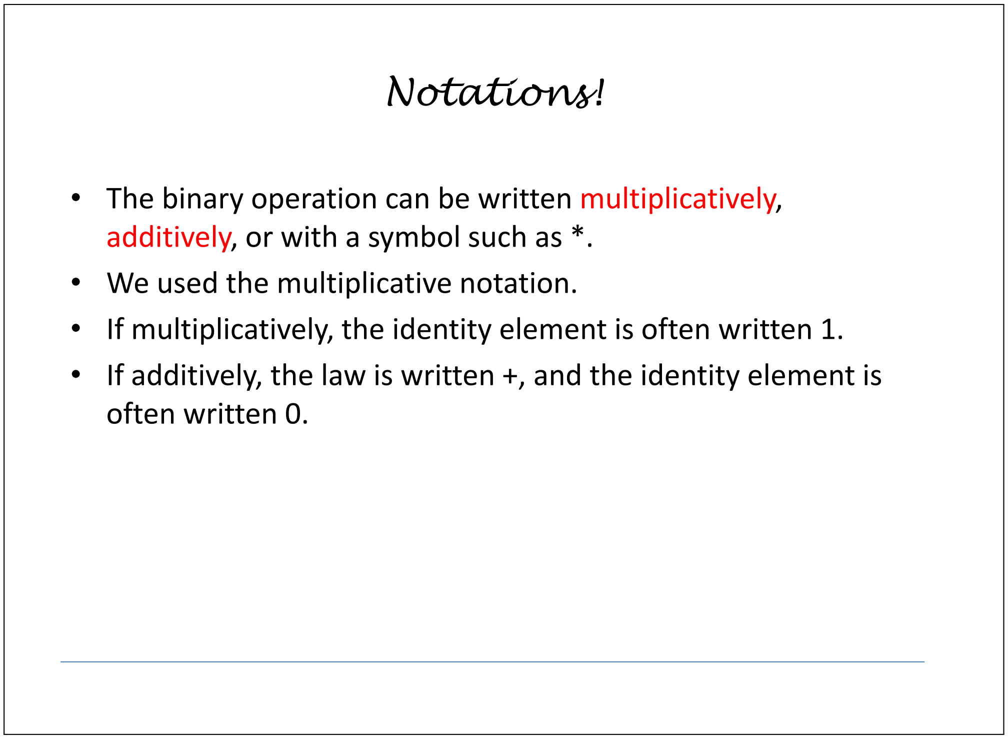


Definition of Group

A **group G** is a set with a binary operation · which maps a pair (g,h) in GxG to g·h in G,

which satisfies:

- The operation is associative, that is to say (f·g)·h=f·(g·h) for any three (not necessarily distinct) elements of G.
- There is an element e in G, called an identity element, such that g·e=g=e·g for every g in G.
- Each element x of G has an inverse g^{-1} which belongs to G and satisfies $g^{-1}\cdot g=e=g\cdot g^{-1}$ ·



Notations!

- The binary operation can be written multiplicatively, additively, or with a symbol such as *.
- We used the multiplicative notation.
- If multiplicatively, the identity element is often written 1.
- If additively, the law is written +, and the identity element is often written 0.

There are many things to comment about this definition! We understand what a set G means. Now we consider this set together with a binary operation (also called binary law). This binary operation can be different things, depending on the nature of the set G. As a result, this operation can be denoted in different ways as well. Let us see some of them. We will write the set and the law as a pair, to make explicit the binary operation:

- In multiplicative notation, we write $(G, \cdot)$, and the identity element is often written 1, or 1_G if several groups and their identity elements are involved.
- In additive notation, we write $(G, +)$, and the identity element is often written 0, or 0_G.
- There could be more general notations, such as $(G, *)$, when we want to emphasize that the operation can be very general.

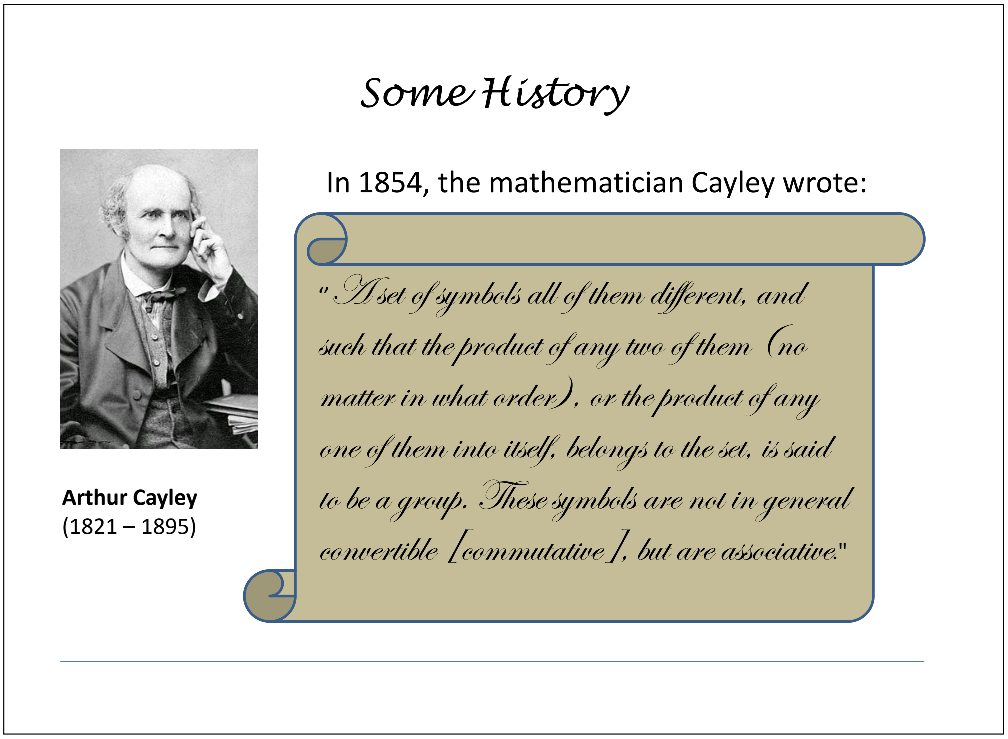
The multiplicative notation *really is* a notation! For example, if m denotes a mirror rotation and r a rotation, the notation $r \cdot m$ (or in fact rm for short) means *the composition of maps*, since multiplying these maps does not make sense! It is thus important to understand the meaning of the formalism that we are using!

There are 4 key properties in the definition of group. Let us use the multiplicative notation here, that is we have a group $(G, \cdot)$.

1. If we take two elements in our group G, let us call them g_1, g_2, then $g_1 \cdot g_2$ must belong to G.
2. The binary operation that we consider must be associative.
3. There must exist an identity element.
4. Every element must have an inverse.

If any of these is not true, then we do not have a group structure.

It is interesting to notice that the modern definition of group that we just saw was in fact proposed by the mathematician Cayley, back in 1854!

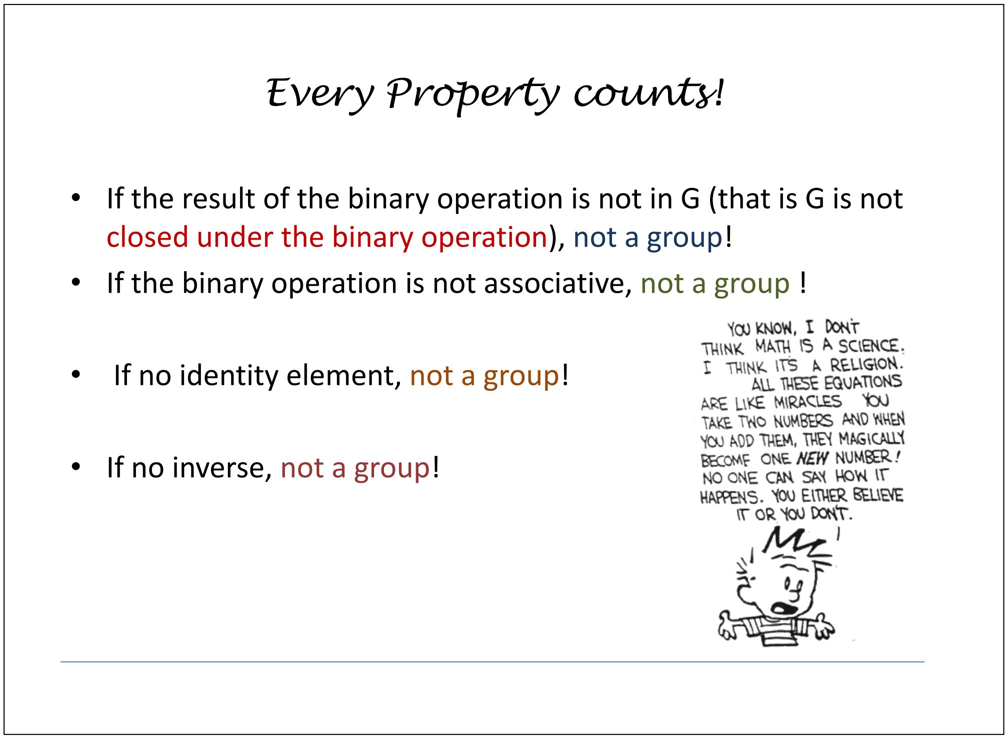


Some History

In 1854, the mathematician Cayley wrote:

> *"A set of symbols all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group. These symbols are not in general convertible [commutative], but are associative."*

Arthur Cayley
(1821 – 1895)



Every Property counts!

- If the result of the binary operation is not in G (that is G is not closed under the binary operation), not a group!
- If the binary operation is not associative, not a group !
- If no identity element, not a group!
- If no inverse, not a group!

YOU KNOW, I DON'T THINK MATH IS A SCIENCE. I THINK IT'S A RELIGION. ALL THESE EQUATIONS ARE LIKE MIRACLES. YOU TAKE TWO NUMBERS AND WHEN YOU ADD THEM, THEY MAGICALLY BECOME ONE NEW NUMBER! NO ONE CAN SAY HOW IT HAPPENS. YOU EITHER BELIEVE IT OR YOU DON'T.

To get used to the formalism of the group definition, let us try to make a small proof.

Proposition 1. *Let $(G, \cdot)$ be a group, with identity element e. Then this identity element is unique.*

Proof. To prove that e is unique, we will assume that there is another identity element e', and show that $e = e'$. Let us thus do so, and assume that both e and e' are identity elements of G.

We now recall what is the definition of an identity element. If e is an identity element, then it must satisfy

$$e \cdot g = g \cdot e = g \tag{3.1}$$

for every element g of G, and e' must similarly satisfy

$$e' \cdot g = g \cdot e' = g \tag{3.2}$$

for every element g of G.

Now we know that (3.1) is true for every element in G, thus it is true for e' as well, and

$$e \cdot e' = e'.$$

We redo the same thing with e'. Because (3.2) is true for every element in G, then it is true for e, which gives

$$e \cdot e' = e.$$

Now we put these two equations together, to obtain

$$e \cdot e' = e' = e \Rightarrow e' = e.$$

□

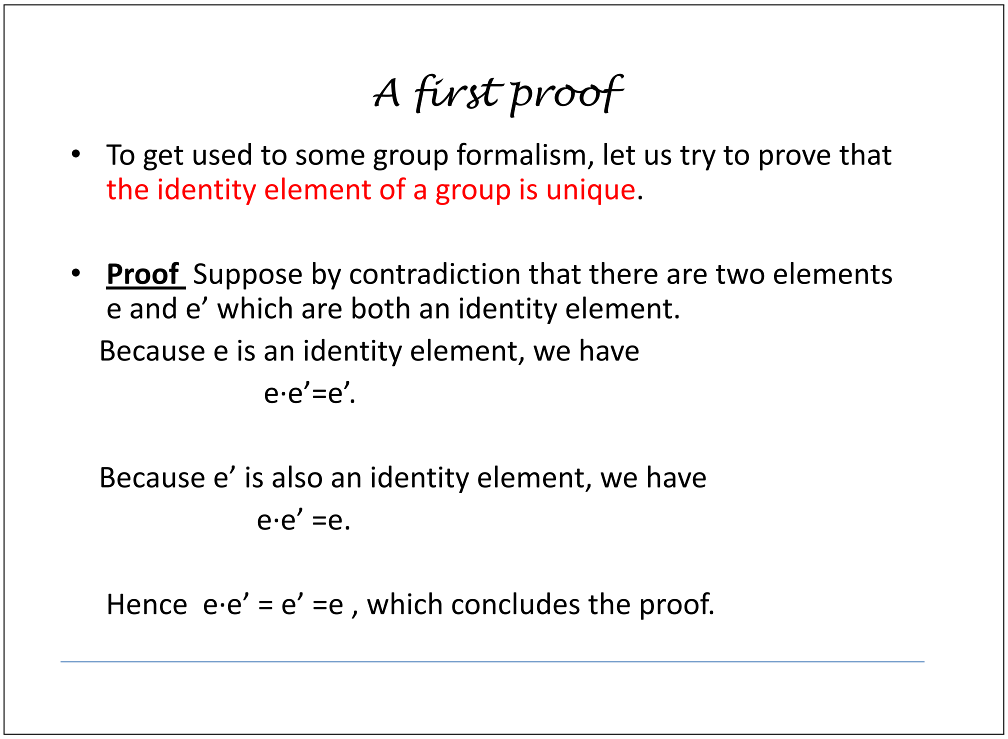
A group becomes much simpler to understand if its binary operation is in fact commutative. We give such groups a particular name.

Definition 5. Let $(G, \cdot)$ be a group. If the binary operation $\cdot$ is commutative, i.e., if we have

$$\forall g_1, g_2 \in G, \quad g_1 \cdot g_2 = g_2 \cdot g_1,$$

then the group is called **commutative** or **abelian** (in honor of the mathematician Abel (1802-1829)).

When a group is abelian, its binary operation is often denoted additively, that is $(G, +)$.



A first proof

- To get used to some group formalism, let us try to prove that the identity element of a group is unique.

- **Proof** Suppose by contradiction that there are two elements e and e’ which are both an identity element.

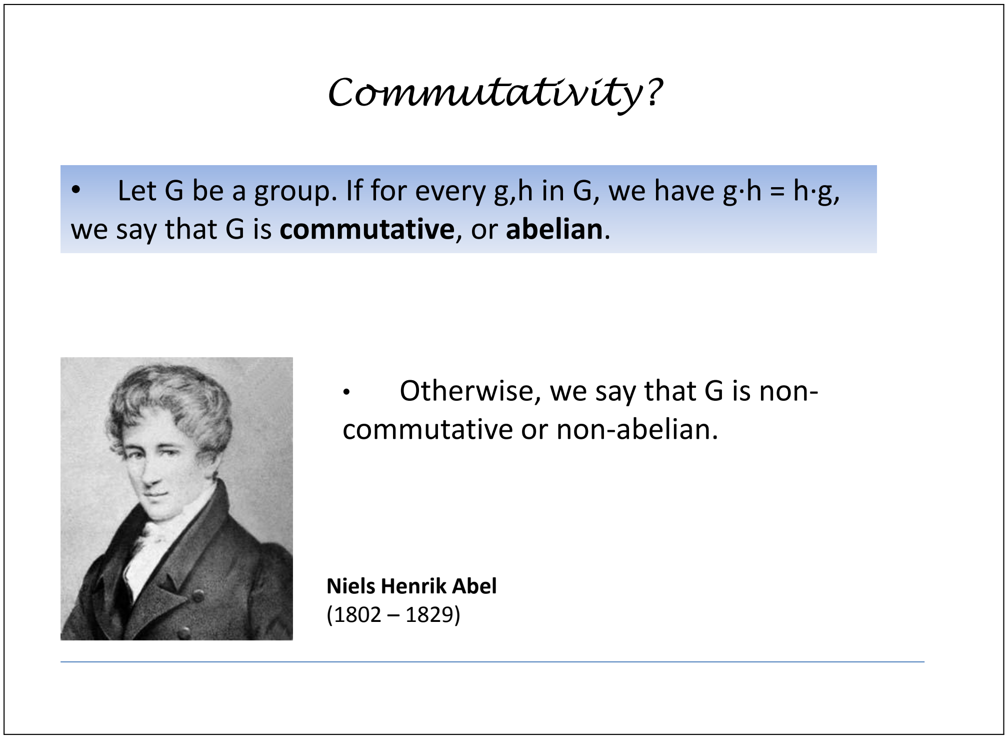
Because e is an identity element, we have

$$e\cdot e'=e'.$$

Because e’ is also an identity element, we have

$$e\cdot e'=e.$$

Hence e·e’ = e’ =e , which concludes the proof.



Commutativity?

- Let G be a group. If for every g,h in G, we have g·h = h·g, we say that G is **commutative**, or **abelian**.

- Otherwise, we say that G is non-commutative or non-abelian.

Niels Henrik Abel
(1802 – 1829)

Suppose we have a group with a given binary operation. We now look at subsets of this group, which also have a group structure with respect to the same binary operation!

Definition 6. If $(G, \cdot)$ is a group and H is a subset of G, so that $(H, \cdot)$ is a group too, we shall call $(H, \cdot)$ a subgroup of G.

Note again that the above definition can be written in additive notation.

We may consider the subgroup $H = G$ as a subgroup of G. Another example of subgroup which is always present in any group G is the *trivial* subgroup formed by the identity element only!

Let us use the multiplicative notation, and let $(G, \cdot)$ be a group with identity element 1. Now we need to check that $H = \{1\}$ is indeed a subgroup of G. It is of course a subset of G, so we are left to check that it has a group structure. Well, all we need to know here is that $1 \cdot 1 = 1$, which is true from the fact that G is a group. This shows at once that (1) combining elements of H gives an element in H, (2) there is an identity element in H, and (3) the element of H is invertible (it is its own inverse in fact). There is no need to check the associativity of the binary law here, since it is inherited from that of G.

If H is a subgroup of G, they are both groups, and the size of H is always smaller or equal to that of G. The size of a group G has a name, we usually refer to it as being the order of the group G.

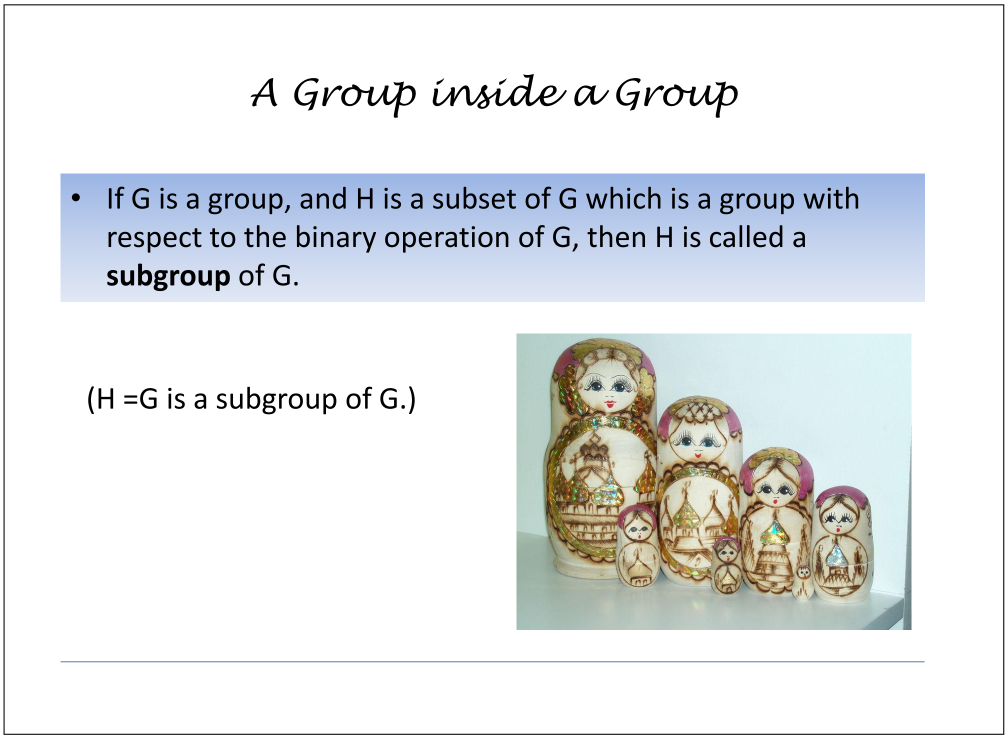
Definition 7. If $(G, \cdot)$ is a group, the number of elements of G (i.e., the cardinality of the set G) is called the order of the group G. It is denoted by $|G|$.

For example, to write formally that the size of a subgroup H of G is always smaller or equal to that of G, we write: $|H| \leq |G|$.

A group G can be finite ($|G| < \infty$) or infinite ($|G| = \infty$)! We will see examples of both types.

> Be careful here: the word “order” means *two different things* in group theory, depending on whether we refer to the order of a group, or to the order of an element!!

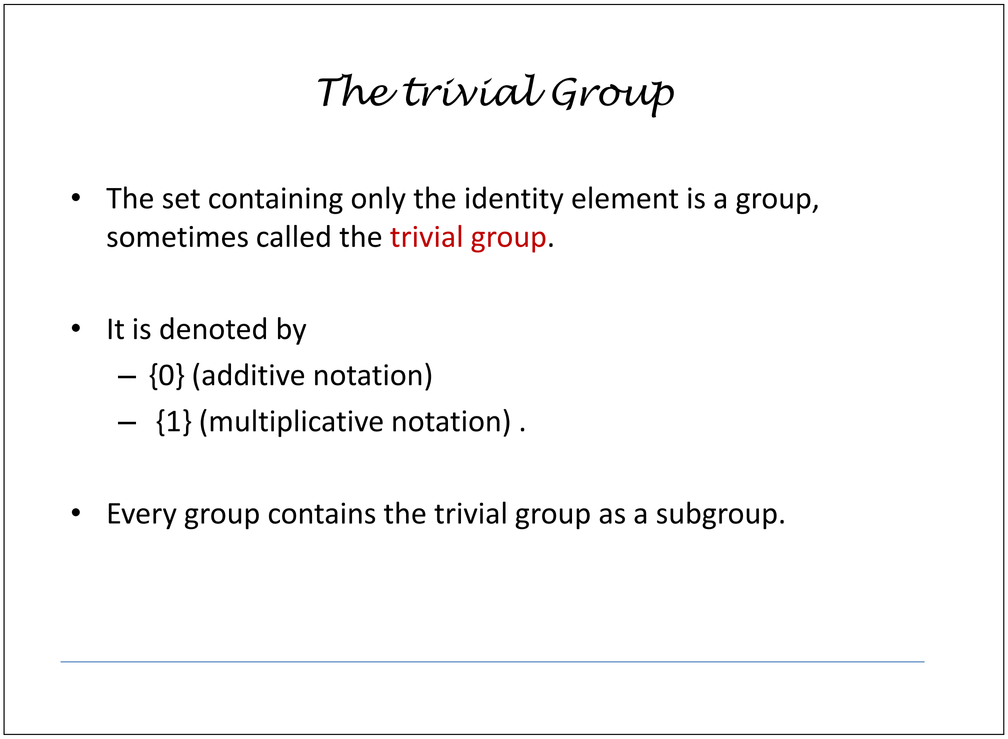
We next define the order of an element in a group.



A Group inside a Group

- If G is a group, and H is a subset of G which is a group with respect to the binary operation of G, then H is called a **subgroup** of G.

(H =G is a subgroup of G.)



The trivial Group

- The set containing only the identity element is a group, sometimes called the trivial group.

- It is denoted by
  - {0} (additive notation)
  - {1} (multiplicative notation) .

- Every group contains the trivial group as a subgroup.

From now on, we will adopt the multiplicative notation, and very often when things are clear enough even remove the $\cdot$ notation. For example, we will write $g_1 g_2$ instead of $g_1 \cdot g_2$.

Definition 8. Let G be a group with identity element e. The order of an element g in G is the **smallest positive integer** k such that

$$\underbrace{ggg \cdots g}_{k\ times} = g^k = e.$$

Note that such a k might not exist! In that case, we will say that g has an infinite order. The notation for the order of an element g varies, it is sometimes denoted by $|g|$, or $o(g)$.

One might wonder why we have two concepts of order, with the same name. It suggests they might be related, and in fact they are, but this is something we will see only later!

Let $(G, \cdot)$ be a group whose order is $|G| = n$, that is G contains a finite number n of elements. Suppose that this group G contains an element g whose order is also n, that is an element g such that

$$g^n = e$$

and there is no smaller positive power k of g such that $g^k = e$. Then

$$g, g^2, \ldots, g^{n-1}, g^n = e$$

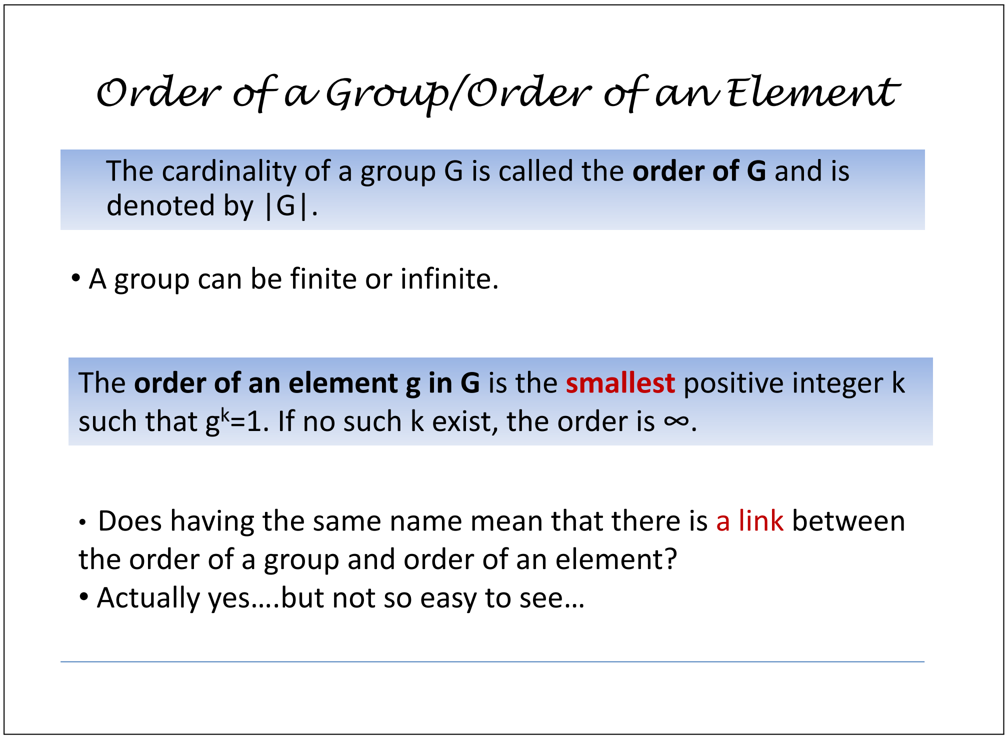
are all distinct elements of G. Indeed should we have some $g^s = g^{s+t}$ for $t < n$ then by multiplying both sides with g^{-s}, we would get that $g^t = 1$ for $t < n$, a contradiction to the minimality of n!

But the group, by assumption, has only n distinct elements, hence we must have that

$$G = \{1, g, g^2, \ldots, g^{n-1}\}.$$

If this is the case, we say that $(G, \cdot)$ is **generated** by g, which we write $G = \langle g \rangle$.

These types of groups are very nice! In fact they are the simplest form of groups that we will encounter. They are called cyclic groups.



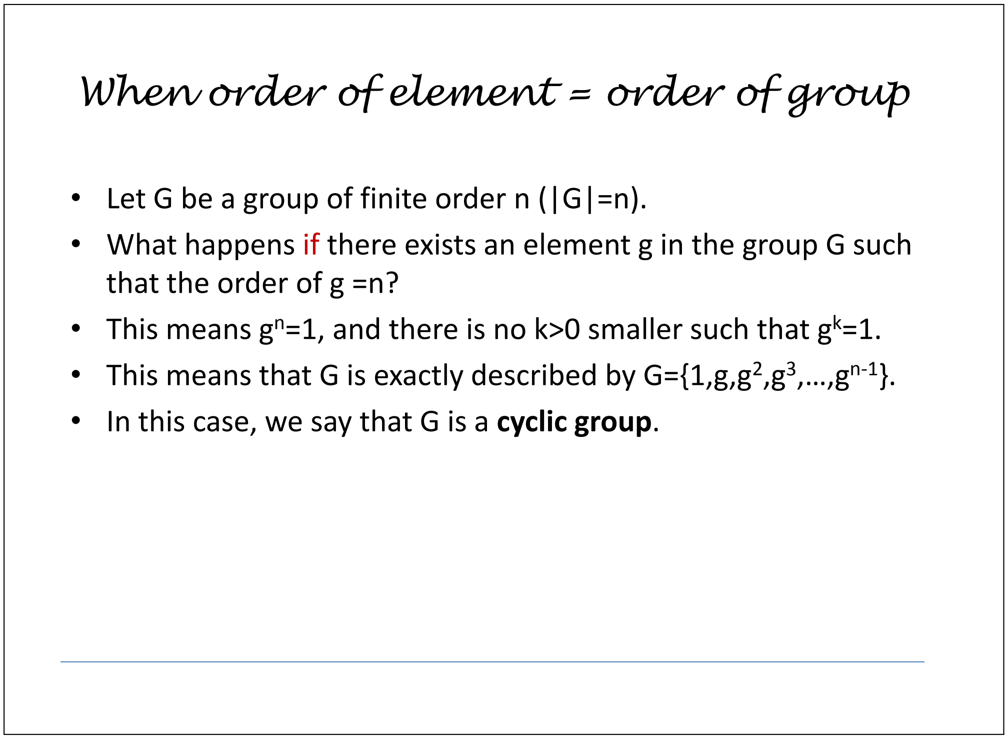
Order of a Group/Order of an Element

The cardinality of a group G is called the **order of G** and is denoted by |G|.

- A group can be finite or infinite.

The **order of an element g in G** is the **smallest** positive integer k such that $g^k=1$. If no such k exist, the order is ∞.

- Does having the same name mean that there is a link between the order of a group and order of an element?
- Actually yes….but not so easy to see…



When order of element = order of group

- Let G be a group of finite order n (|G|=n).
- What happens if there exists an element g in the group G such that the order of g =n?
- This means $g^n=1$, and there is no k>0 smaller such that $g^k=1$.
- This means that G is exactly described by $G=\{1,g,g^2,g^3,\ldots,g^{n-1}\}$.
- In this case, we say that G is a **cyclic group**.

Definition 9. A group G will be called cyclic if it is generated by an element g of G, i.e.,

$$G = \langle g \rangle = \{g^m | m \in \mathbb{Z}\}.$$

Notice that this definition covers both the case of a finite cyclic group (in that case, $g^n = e$ for some n, and this set is indeed finite) and of an infinite cyclic group.

To start with, cyclic groups have this nice property of being abelian groups.

Proposition 2. *Cyclic groups are abelian.*

Proof. To show that a group is abelian, we have to show that

$$g_1 g_2 = g_2 g_1$$

for any choice of elements g_1 and g_2 in G. Now let G be a cyclic group. By definition, we know that G is generated by a single element g, that is

$$G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}.$$

Thus both g_1 and g_2 can be written as a power of g:

$$g_1 = g^i, \ g_2 = g^j$$

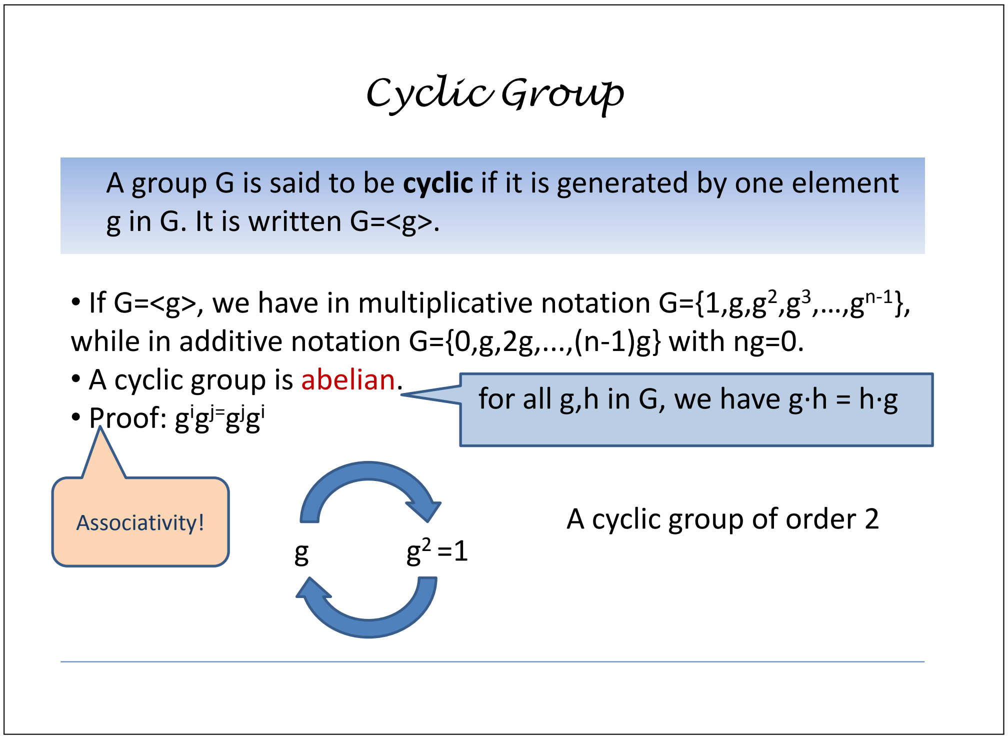
for some power i and j, and thus, thanks to the associativity of the binary operation

$$g_1 g_2 = g^i g^j = g^{i+j} = g^j g^i = g_2 g_1$$

which concludes the proof. □

Let us summarize what we have been doing so far in this chapter.

- We defined this abstract notion of group.
- Using it, we defined more abstract things: an abelian group, the order of a group, the order of an element of a group, the notion of subgroup, and that of cyclic group.
- We also saw that based only on these definitions, we can start proving results, such as the uniqueness of the identity element, or the fact that cyclic groups are abelian.



Cyclic Group

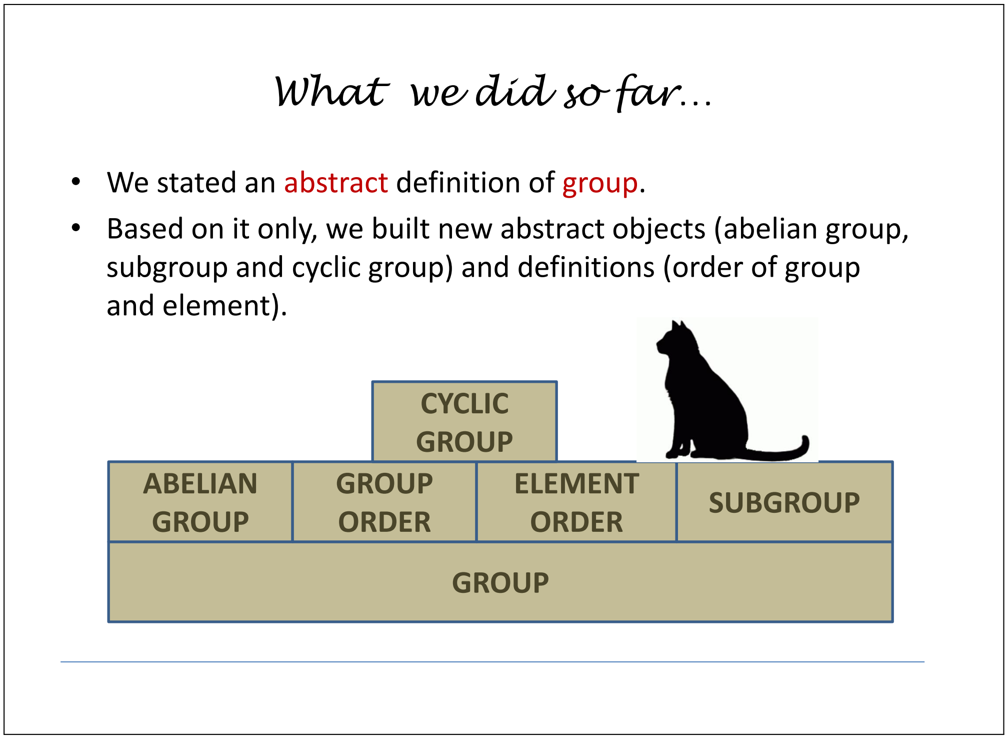
A group G is said to be **cyclic** if it is generated by one element g in G. It is written G=<g>.

- If G=<g>, we have in multiplicative notation G={1,g,g^2,g^3,…,g^{n-1}}, while in additive notation G={0,g,2g,...,(n-1)g} with ng=0.
- A cyclic group is abelian.
- Proof: $g^i g^j = g^j g^i$

for all g,h in G, we have g·h = h·g

Associativity!

A cyclic group of order 2



What we did so far…

- We stated an abstract definition of group.
- Based on it only, we built new abstract objects (abelian group, subgroup and cyclic group) and definitions (order of group and element).

CYCLIC GROUP
ABELIAN GROUP
GROUP ORDER
ELEMENT ORDER
SUBGROUP
GROUP

This might look really abstract, which is somewhat normal since this is a first step into abstract algebra. However, you already know all these abstract objects, because you saw them already in the two previous chapters! These definitions are abstracting mathematical properties that we observed. We will spend the rest of this chapter to convince you that this is indeed the case.

We will use a lot the notion of multiplication table for the rest of this chapter. We note that they are sometimes called *Cayley tables*.

Recall from the previous chapter that we have obtained the complete set of symmetries for a rectangle, whose multiplication table we recall below (we write $m = m_v$ for the vertical mirror reflection):

	1	m	r_π	mr_π
1	1	m	r_π	mr_π
m	m	1	mr_π	r_π
r_π	r_π	mr_π	1	m
mr_π	mr_π	r_π	m	1

First of all, let us see that the symmetries of a rectangle form a group G, with respect to the binary operation given by the composition of maps.

- Composition of symmetries yields another symmetry (this can be observed from the multiplication table).

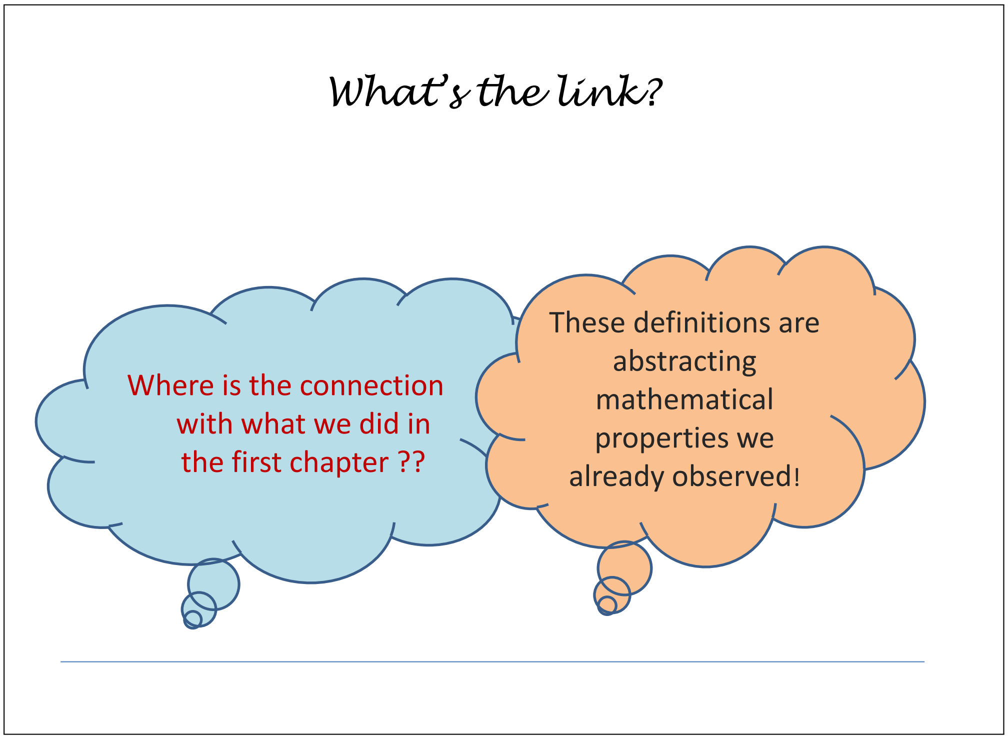
- Composition of symmetries is associative.

- There exists an identity element, the identity map 1.

- Each element has an inverse (itself!) This can be seen from the table as well!

This shows that the set of symmetries of a rectangle forms a group. Note that this group is abelian, which can be seen from the fact that the multiplication table is symmetric w.r.t. the main diagonal.

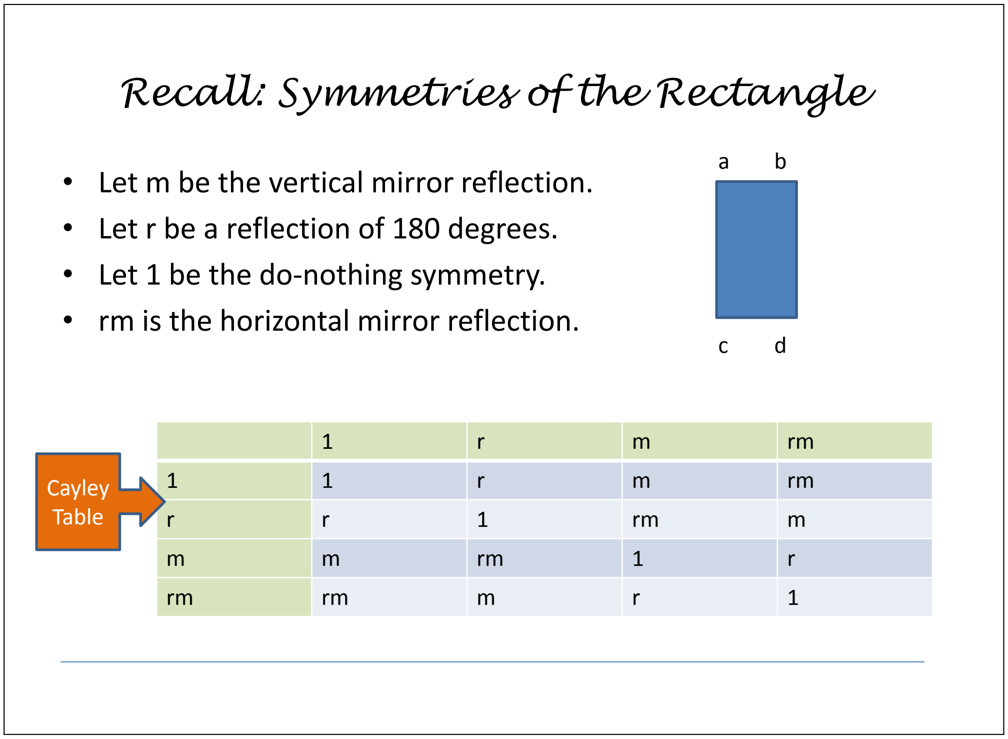
Of course, that the set of symmetries of a rectangle forms an abelian group can be shown without computing a multiplication table, but since we know it, it gives an easy way to visualize the group structure.



What's the link?

Where is the connection with what we did in the first chapter ??

These definitions are abstracting mathematical properties we already observed!



Recall: Symmetries of the Rectangle

- Let m be the vertical mirror reflection.
- Let r be a reflection of 180 degrees.
- Let 1 be the do-nothing symmetry.
- rm is the horizontal mirror reflection.

Cayley Table

	1	r	m	rm
1	1	r	m	rm
r	r	1	rm	m
m	m	rm	1	r
rm	rm	m	r	1

The group of symmetries of the rectangle has order 4.

Let us look at the order of the elements:

$$m^2 = 1,\ r^2 = 1,\ (rm)^2 = 1,$$

thus these elements have order 2.

We next look at the subgroups:

- The trivial subgroup $\{1\}$ is here.
- We have that $\{1, r\}$ forms a subgroup of order 2.
- Similarly $\{1, m\}$ forms a subgroup of order 2.
- Finally $\{1, rm\}$ also forms a subgroup of order 2.

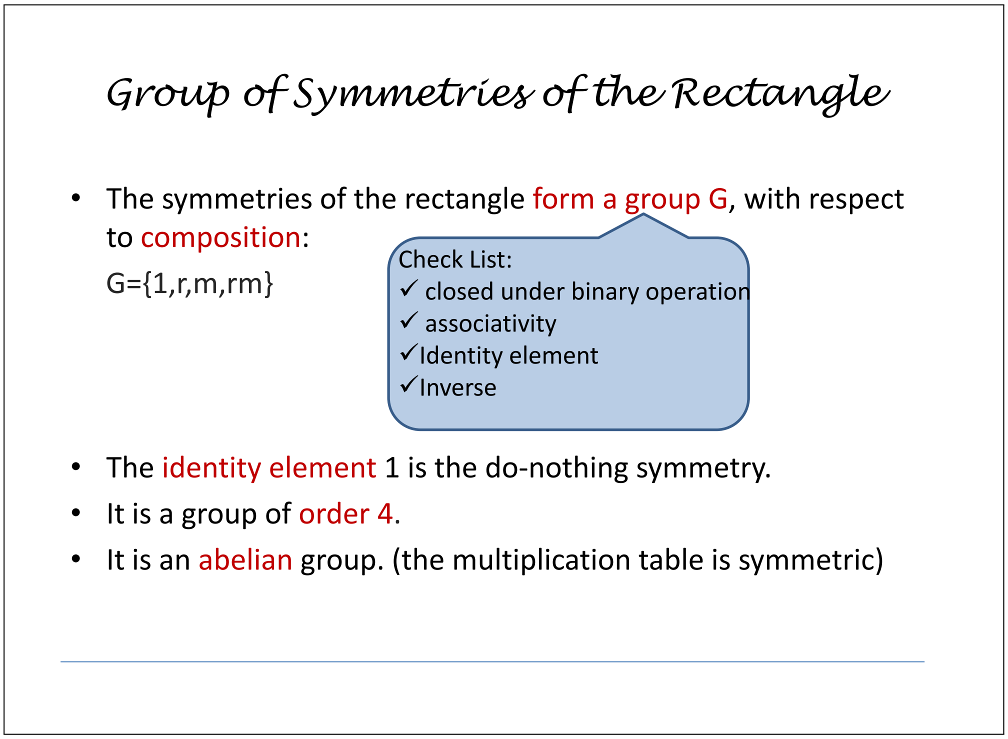
We can observe that these are the only subgroups, since by adding a 3rd element to any of them, we will get the whole group! Let us illustrate this claim with an example. Let us try to add to $\{1, r\}$, say m. We get $H = \{1, r, m\}$ but for this set H to be a group, we need to make sure that the composition of any two maps is in H! Clearly rm is not, so we need to add it if we want to get a group, but then we get G!

We further note that all the subgroups are cyclic subgroups! For example, $\{1, m\} = \langle m \rangle$. But G itself is not a cyclic group, since it contains no element of order 4.

Let us summarize our findings:

Let G be the group of symmetries of the rectangle.

1. It is an **abelian** group of **order 4**.
2. Apart from the identity element, it contains 3 elements of order 2.
3. It is **not a cyclic** group.
4. It contains 3 cyclic subgroups of order 2.



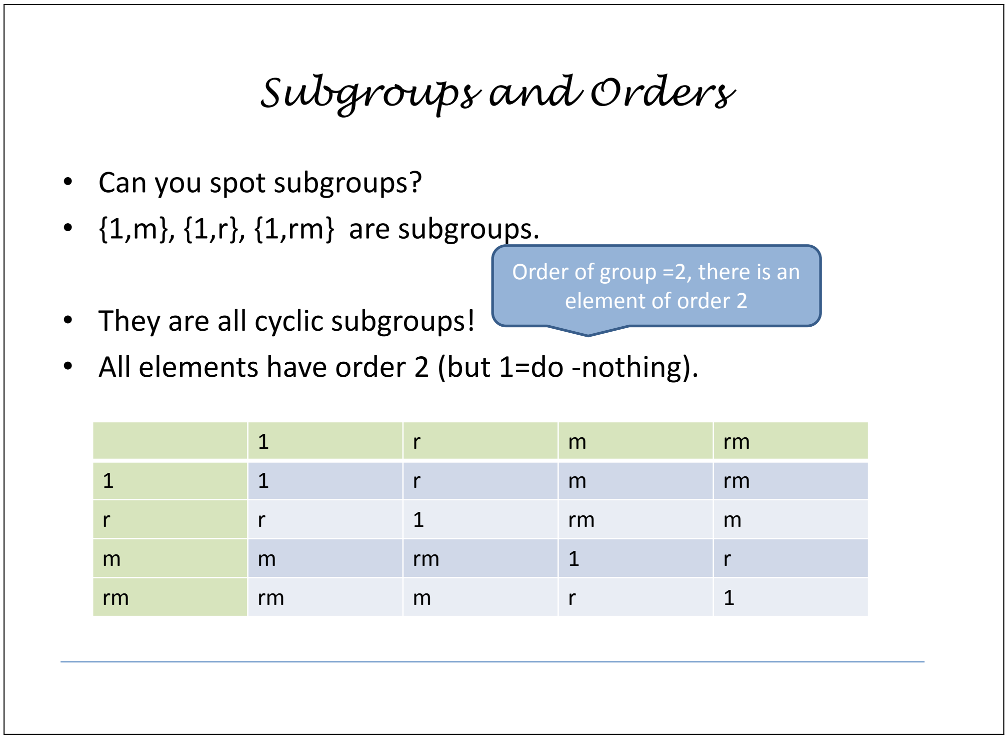
Group of Symmetries of the Rectangle

- The symmetries of the rectangle form a group G, with respect to composition:

  G={1,r,m,rm}

Check List:
✓ closed under binary operation
✓ associativity
✓Identity element
✓Inverse

- The identity element 1 is the do-nothing symmetry.
- It is a group of order 4.
- It is an abelian group. (the multiplication table is symmetric)



Subgroups and Orders

- Can you spot subgroups?
- {1,m}, {1,r}, {1,rm} are subgroups.

Order of group =2, there is an element of order 2

- They are all cyclic subgroups!
- All elements have order 2 (but 1=do -nothing).

	1	r	m	rm
1	1	r	m	rm
r	r	1	rm	m
m	m	rm	1	r
rm	rm	m	r	1

Let us now look at our second example, the symmetries of the square. We recall that there are 8 symmetries:

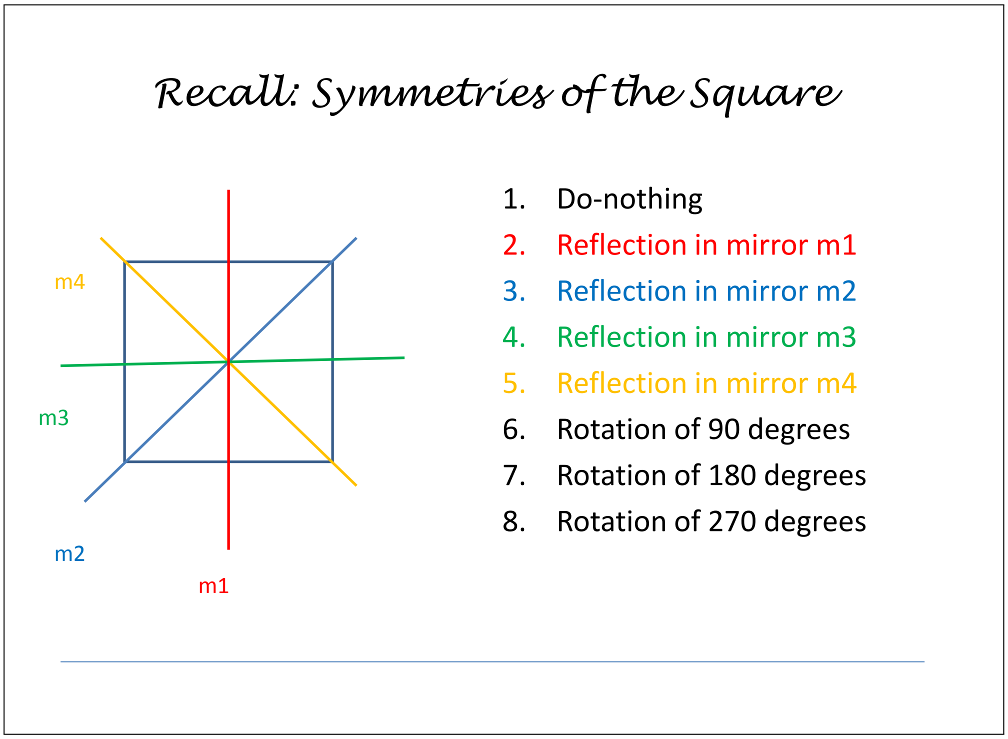
1. m_1= reflection with respect to the y-axis,
2. m_2= reflection with respect to the line $y = x$,
3. m_3= reflection with respect to the x-axis,
4. m_4= reflection with respect to the line $y = -x$,
5. the rotation $r_{\pi/2}$,
6. the rotation r_π,
7. the rotation $r_{3\pi/2}$,
8. and of course the identity map 1!

By fixing $m = m_3$ and $r = r_{3\pi/2}$, we also computed that

$$\begin{aligned} rm &= m_4 \\ r^2m &= m_1 \\ r^3m &= m_2 \end{aligned}$$

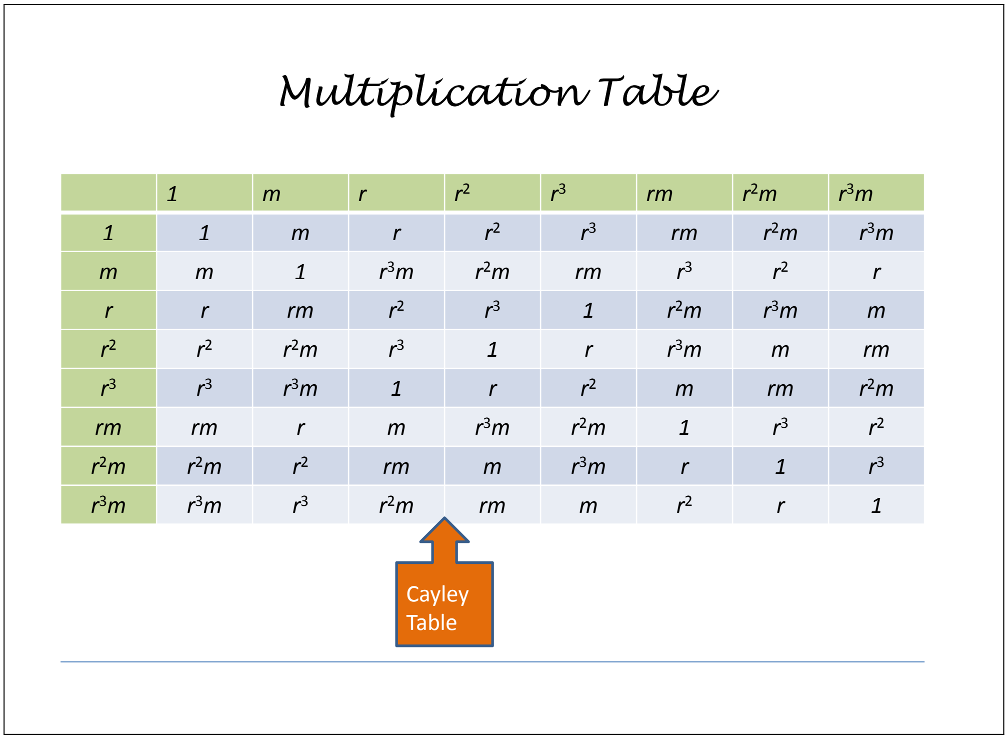
which allowed us to compute the following multiplication (Cayley) table.

	1	m	r	r^2	r^3	rm	r^2m	r^3m
1	1	m	r	r^2	r^3	rm	r^2m	r^3m
m	m	1	r^3m	r^2m	rm	r^3	r^2	r
r	r	rm	r^2	r^3	1	r^2m	r^3m	m
r^2	r^2	r^2m	r^3	1	r	r^3m	m	rm
r^3	r^3	r^3m	1	r	r^2	m	rm	r^2m
rm	rm	r	m	r^3m	r^2m	1	r^3	r^2
r^2m	r^2m	r^2	rm	m	r^3m	r	1	r^3
r^3m	r^3m	r^3	r^2m	rm	m	r^2	r	1



Recall: Symmetries of the Square

1. Do-nothing
2. Reflection in mirror m1
3. Reflection in mirror m2
4. Reflection in mirror m3
5. Reflection in mirror m4
6. Rotation of 90 degrees
7. Rotation of 180 degrees
8. Rotation of 270 degrees



Multiplication Table

	1	m	r	r^2	r^3	rm	r^2m	r^3m
1	1	m	r	r^2	r^3	rm	r^2m	r^3m
m	m	1	r^3m	r^2m	rm	r^3	r^2	r
r	r	rm	r^2	r^3	1	r^2m	r^3m	m
r^2	r^2	r^2m	r^3	1	r	r^3m	m	rm
r^3	r^3	r^3m	1	r	r^2	m	rm	r^2m
rm	rm	r	m	r^3m	r^2m	1	r^3	r^2
r^2m	r^2m	r^2	rm	m	r^3m	r	1	r^3
r^3m	r^3m	r^3	r^2m	rm	m	r^2	r	1

Cayley Table

Let us check that the symmetries of the square form a group. We consider the set

$$G = \{1, r, r^2, r^3, m, mr, mr^2, mr^3\}$$

together with the composition of maps as binary law. Then we have

- closure under the binary composition, that is the composition of two symmetries is again a symmetry,
- the composition is associative,
- there exists an identity element,
- each element has an inverse (this can be seen in the table, since every row has a 1!)

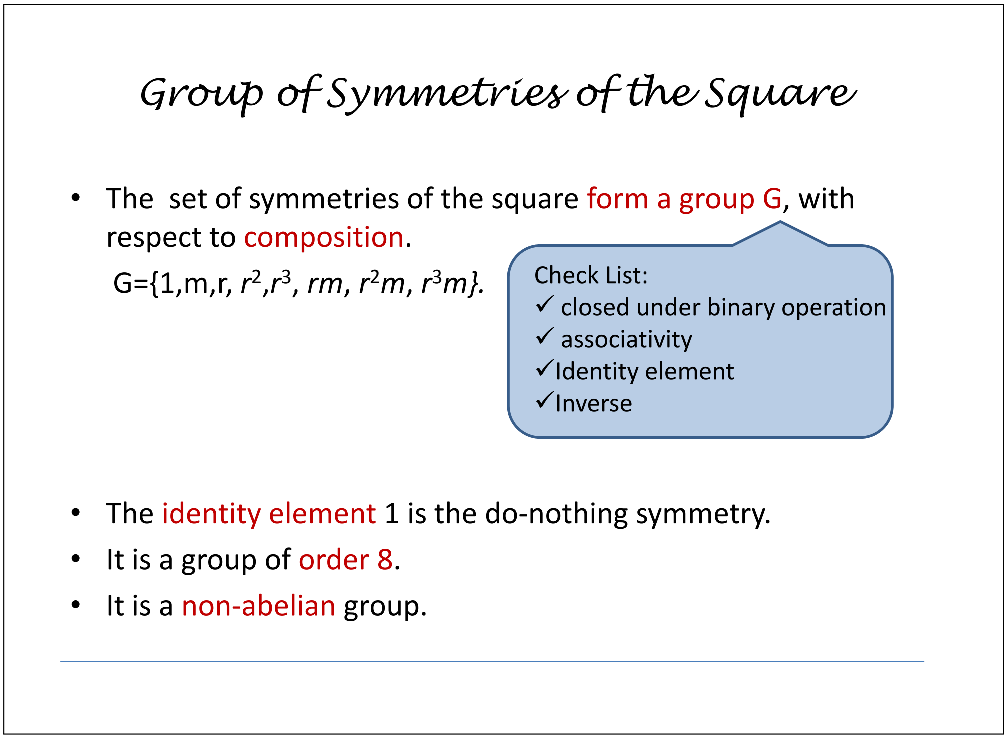
We just showed that G is a group.

It is a group of order 8, which is not abelian, since $rm \neq mr$. Note that as a result G cannot be cyclic, since we proved that every cyclic group is abelian!

We next look at possible subgroups of G. Let us try to spot some of them.

- We have that $\{1, m\}$ forms a subgroup of order 2. It contains an element m of order 2, thus it is cyclic!
- Another subgroup can be easily spotted by reordering the rows and columns of the Cayley table. This is $\{1, r, r^2, r^3\}$, which is a subgroup of order 4. It contains one element of order 4, that is r, and thus it is cyclic as well! It also contains one element of order 2, that is r^2. The element r^3 also has order 4.
- The subgroup $\{1, r, r^2, r^3\}$ itself contains another subgroup of order 2, given by $\{1, r^2\}$, which is cyclic of order 2.

We have now spotted the most obvious subgroups, let us see if we missed something.



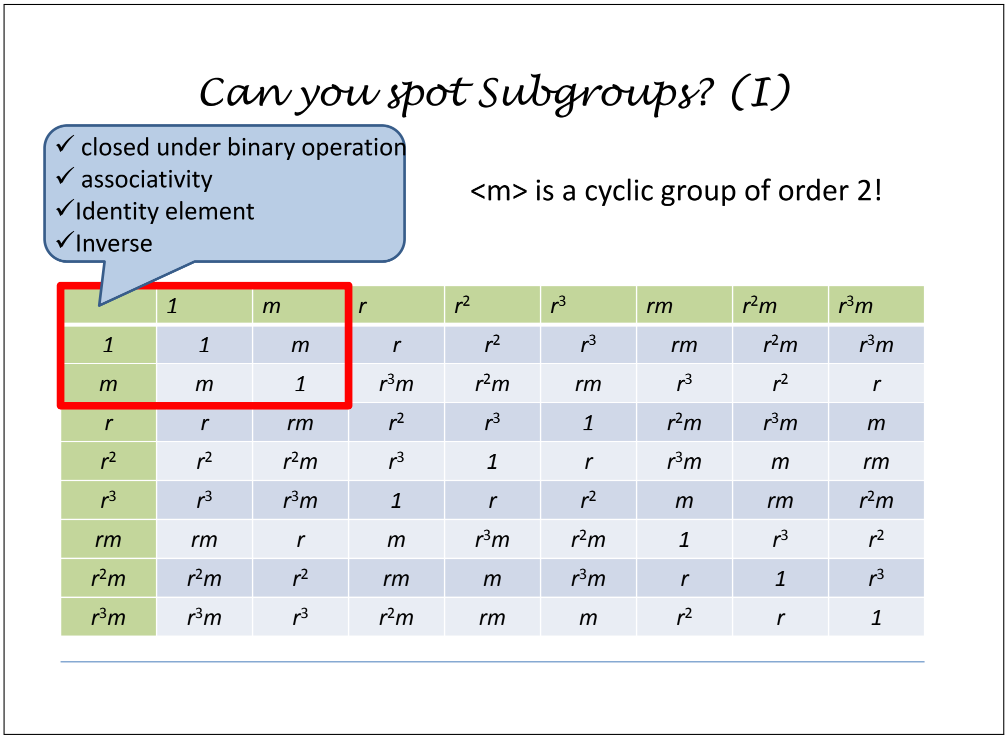
Group of Symmetries of the Square

- The set of symmetries of the square form a group G, with respect to composition.

  G={1,m,r, r^2,r^3, rm, r^2m, r^3m}.

Check List:
✓ closed under binary operation
✓ associativity
✓ Identity element
✓ Inverse

- The identity element 1 is the do-nothing symmetry.
- It is a group of order 8.
- It is a non-abelian group.



Can you spot Subgroups? (I)

✓ closed under binary operation
✓ associativity
✓ Identity element
✓ Inverse

<m> is a cyclic group of order 2!

	1	m	r	r^2	r^3	rm	r^2m	r^3m
1	1	m	r	r^2	r^3	rm	r^2m	r^3m
m	m	1	r^3m	r^2m	rm	r^3	r^2	r
r	r	rm	r^2	r^3	1	r^2m	r^3m	m
r^2	r^2	r^2m	r^3	1	r	r^3m	m	rm
r^3	r^3	r^3m	1	r	r^2	m	rm	r^2m
rm	rm	r	m	r^3m	r^2m	1	r^3	r^2
r^2m	r^2m	r^2	rm	m	r^3m	r	1	r^3
r^3m	r^3m	r^3	r^2m	rm	m	r^2	r	1

If we take the subgroup $\{1, r, r^2, r^3\}$ and try to add one more element, say m, we realize that rm, r^2m,... must be there as well, and thus we get the whole group G.

Let us try to add some more elements to the subgroup $\{1, m\}$. If we add r, then we need to add all the power of r, and we obtain the whole group G again.

Alternatively we could try to add r^2 to $\{1, m\}$. Then we get $H = \{1, m, r^2, r^2m, mr^2\}$, and this we have that $r^2m = mr^2$. Thus we managed to find another subgroup, this time of order 4. It contains 3 elements of order 2.

We had identified the subgroup $\{1, r^2\}$. If we add m, we find the subgroup H again. If we add rm, we find another subgroup given by $\{1, r^2, rm, r^3m\}$.

Finally, we had mentioned at the beginning that $\{1, m\}$ forms a subgroup of order 2. But this is true for every mirror reflection, and we have more than one such reflection: we know we have 4 of them! Thus to each of them corresponds a cyclic subgroup of order 2.

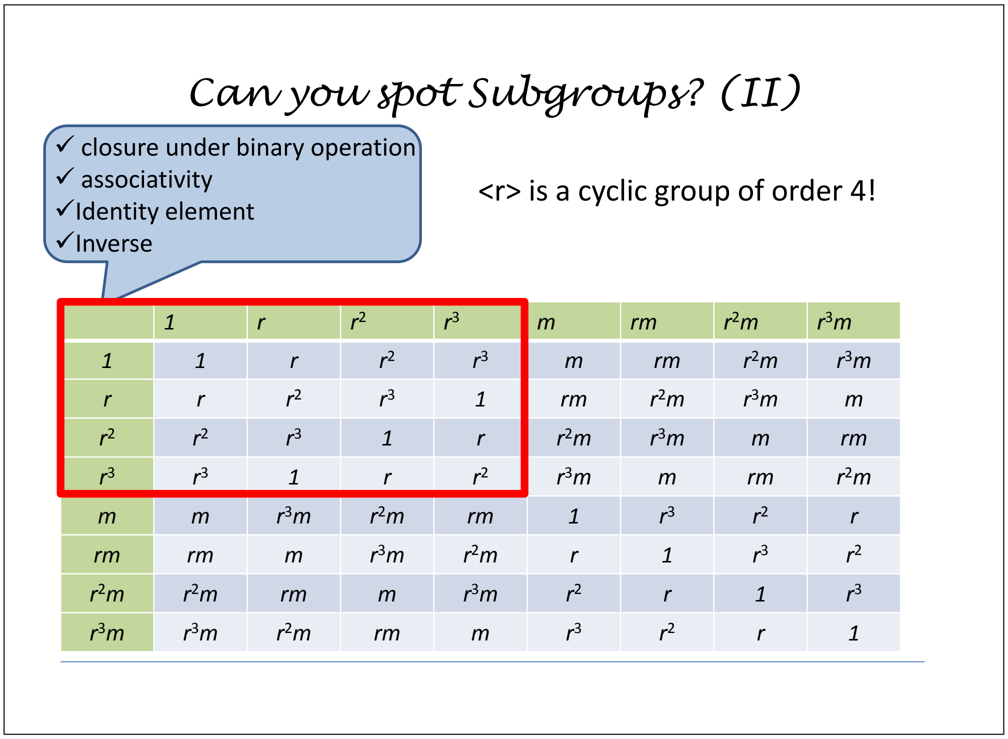
We list all the subgroups of G that we found.

Let G be the group of symmetries of the square. Here is a list of its subgroups.

1. Order 1: the trivial subgroup $\{1\}$.
2. Order 2: the cyclic groups generated by the 4 reflections, that is $\{1, m\}$, $\{1, rm\}$, $\{1, r^2m\}$ and $\{1, r^3m\}$, together with $\{1, r^2\}$.
3. Order 4: we have $\{1, r, r^2, r^3\}$ which is cyclic, and $\{1, m, r^2, r^2m, mr^2\}$ together with $\{1, r^2, rm, r^3m\}$ which are not cyclic.

It is interesting to recognize the group of symmetries of the rectangle, which makes sense, since a square is a special rectangle.

You are right to think that finding all these subgroups is tedious! In fact, finding the list of all subgroups of a given group in general is really hard. However there is nothing to worry about here, since we will not try for bigger groups, and for the symmetries of the square, it was still manageable.

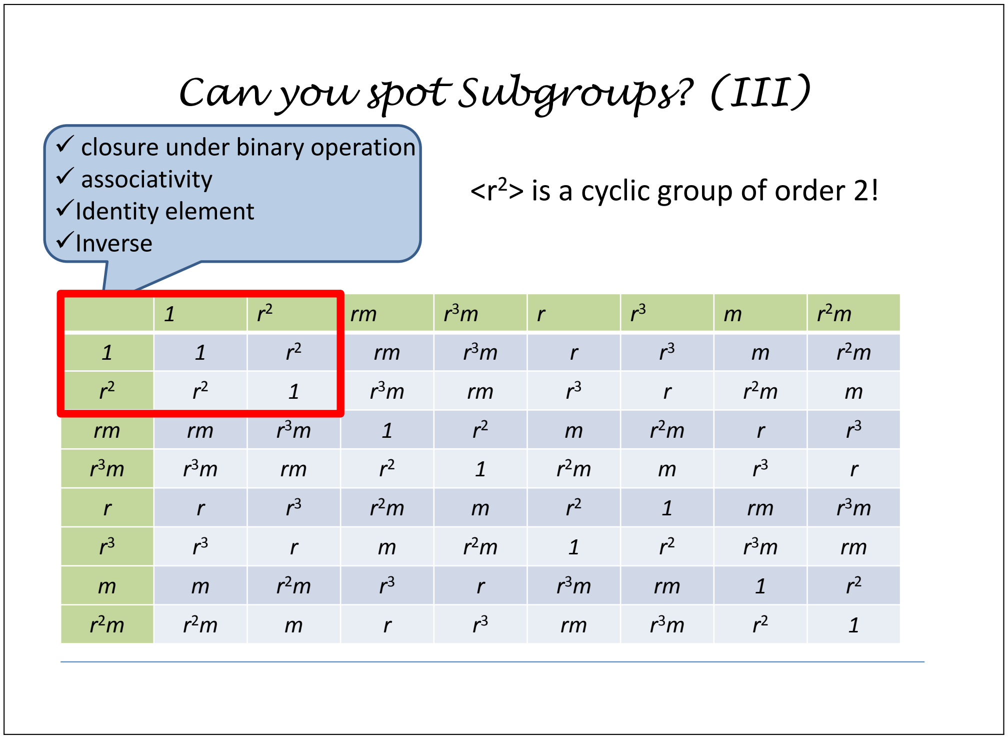


Can you spot Subgroups? (II)

- ✓ closure under binary operation
- ✓ associativity
- ✓Identity element
- ✓Inverse

<r> is a cyclic group of order 4!

	1	r	r^2	r^3	m	rm	r^2m	r^3m
1	1	r	r^2	r^3	m	rm	r^2m	r^3m
r	r	r^2	r^3	1	rm	r^2m	r^3m	m
r^2	r^2	r^3	1	r	r^2m	r^3m	m	rm
r^3	r^3	1	r	r^2	r^3m	m	rm	r^2m
m	m	r^3m	r^2m	rm	1	r^3	r^2	r
rm	rm	m	r^3m	r^2m	r	1	r^3	r^2
r^2m	r^2m	rm	m	r^3m	r^2	r	1	r^3
r^3m	r^3m	r^2m	rm	m	r^3	r^2	r	1



Can you spot Subgroups? (III)

- ✓ closure under binary operation
- ✓ associativity
- ✓Identity element
- ✓Inverse

<r^2> is a cyclic group of order 2!

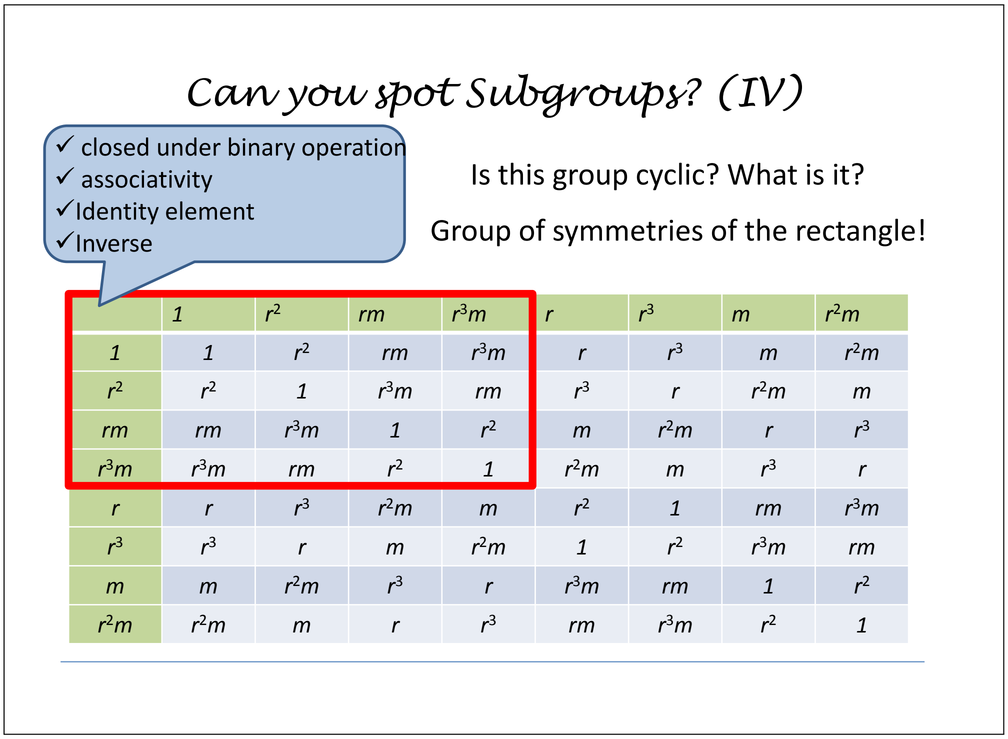
	1	r^2	rm	r^3m	r	r^3	m	r^2m
1	1	r^2	rm	r^3m	r	r^3	m	r^2m
r^2	r^2	1	r^3m	rm	r^3	r	r^2m	m
rm	rm	r^3m	1	r^2	m	r^2m	r	r^3
r^3m	r^3m	rm	r^2	1	r^2m	m	r^3	r
r	r	r^3	r^2m	m	r^2	1	rm	r^3m
r^3	r^3	r	m	r^2m	1	r^2	r^3m	rm
m	m	r^2m	r^3	r	r^3m	rm	1	r^2
r^2m	r^2m	m	r	r^3	rm	r^3m	r^2	1

We finish this example by summarizing all that we found about the group of symmetries of the square.

Let G be the group of symmetries of the square.

1. It is a group of **order 8**.
2. Apart from the identity element, it contains 7 elements, 5 of order 2, and 2 of order 4.
3. It is **not a cyclic** group.
4. In fact, it is **not even an abelian** group.
5. It contains 5 cyclic subgroups of order 2, 1 cyclic subgroup of order 4, and 2 subgroups of order 4 which are not cyclic, for a total of 8 non-trivial subgroups.

In the first two chapters, we explained mathematically nice geometric structures using the notion of symmetries. What we saw in this chapter is that symmetries in fact have a nice algebraic structure, that of a group. What we will do next is study more about groups! Once we have learnt more, we will come back to symmetries again, and see that we can get a much better understanding thanks to some group theory knowledge.



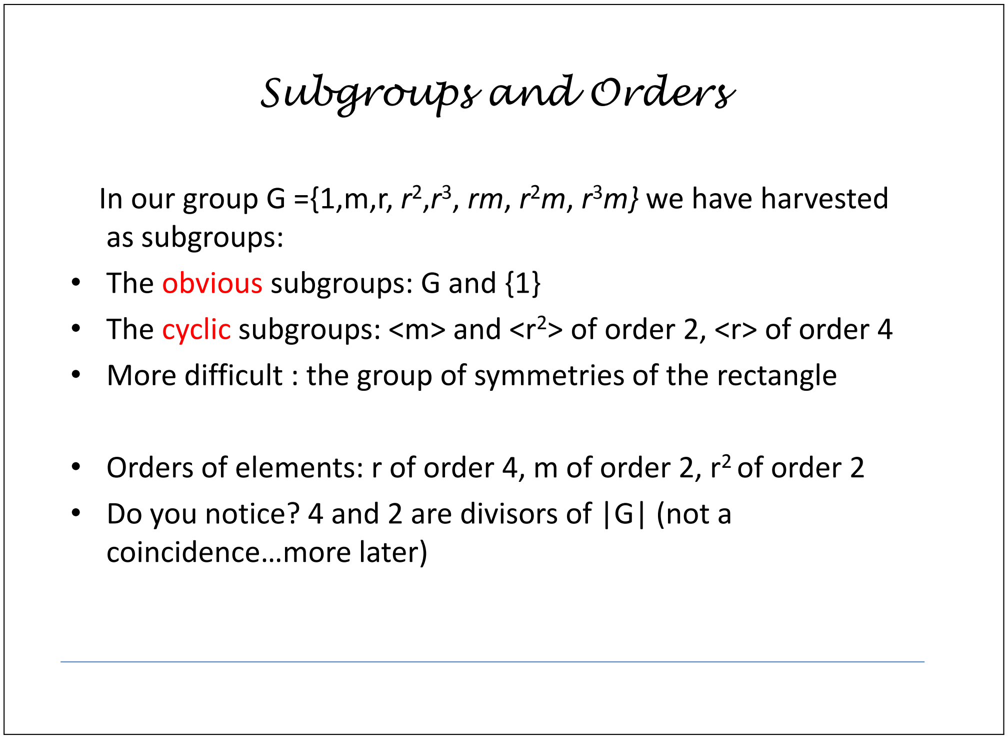
Can you spot Subgroups? (IV)

✓ closed under binary operation
✓ associativity
✓Identity element
✓Inverse

Is this group cyclic? What is it?

Group of symmetries of the rectangle!

	1	r^2	rm	r^3m	r	r^3	m	r^2m
1	1	r^2	rm	r^3m	r	r^3	m	r^2m
r^2	r^2	1	r^3m	rm	r^3	r	r^2m	m
rm	rm	r^3m	1	r^2	m	r^2m	r	r^3
r^3m	r^3m	rm	r^2	1	r^2m	m	r^3	r
r	r	r^3	r^2m	m	r^2	1	rm	r^3m
r^3	r^3	r	m	r^2m	1	r^2	r^3m	rm
m	m	r^2m	r^3	r	r^3m	rm	1	r^2
r^2m	r^2m	m	r	r^3	rm	r^3m	r^2	1



Subgroups and Orders

In our group G ={1,m,r, r^2,r^3, rm, r^2m, r^3m} we have harvested as subgroups:

- The obvious subgroups: G and {1}
- The cyclic subgroups: <m> and <r^2> of order 2, <r> of order 4
- More difficult : the group of symmetries of the rectangle

- Orders of elements: r of order 4, m of order 2, r^2 of order 2
- Do you notice? 4 and 2 are divisors of |G| (not a coincidence…more later)

Exercises for Chapter 3

Exercise 8. In Exercise 5, you determined the symmetries of an equilateral triangle, and computed the multiplication table of all its symmetries. Show that the symmetries of an equilateral triangle form a group.

1. Is it abelian or non-abelian?
2. What is the order of this group?
3. Compute the order of its elements.
4. Is this group cyclic?
5. Can you spot some of its subgroups?

Exercise 9. Let $z = e^{2i\pi/3}$. Show that $\{1, z, z^2\}$ forms a group.

1. Is it abelian or non-abelian?
2. What is the order of this group?
3. Compute the order of its elements.
4. Is this group cyclic?
5. Can you spot some of its subgroups?

Exercise 10. Let X be a metric space equipped with a distance d.

1. Show that the set of bijective isometries of X (with respect to the distance d) forms a group denoted by G.
2. Let S be a subset of X. Define a symmetry of S as an isometry of X that maps S into itself. Show that the set of symmetries of S is a subgroup of G.

Exercise 11. Let G be a group. Show that right and left cancellation laws hold (with respect to the binary group operation), namely:

$$g_2 \cdot g_1 = g_3 \cdot g_1 \Rightarrow g_2 = g_3,$$

$$g_3 \cdot g_1 = g_3 \cdot g_2 \Rightarrow g_1 = g_2,$$

for any $g_1, g_2, g_3 \in G$.