USACH. Santiago, Chile 5 - 9 de Junio, 2023

Introduction to group theory

Pere Alemany
Universitat de Barcelona

The Erlangen program

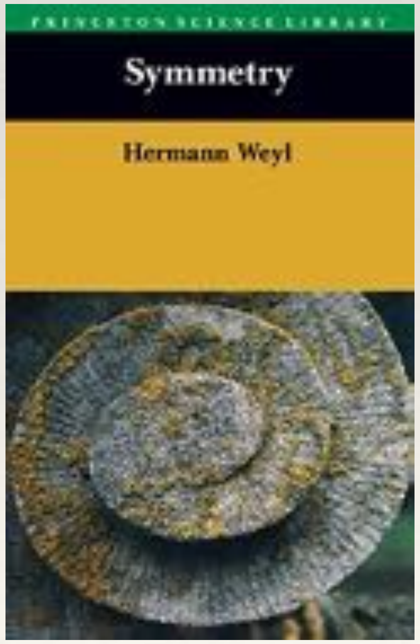
Felix Klein, 1849 - 1925

In 1872 Felix Klein proposed that **group theory**, a branch of mathematics that uses **algebraic methods to abstract the idea of symmetry**, was the most useful way of organizing geometrical knowledge.

Modern definition of symmetry

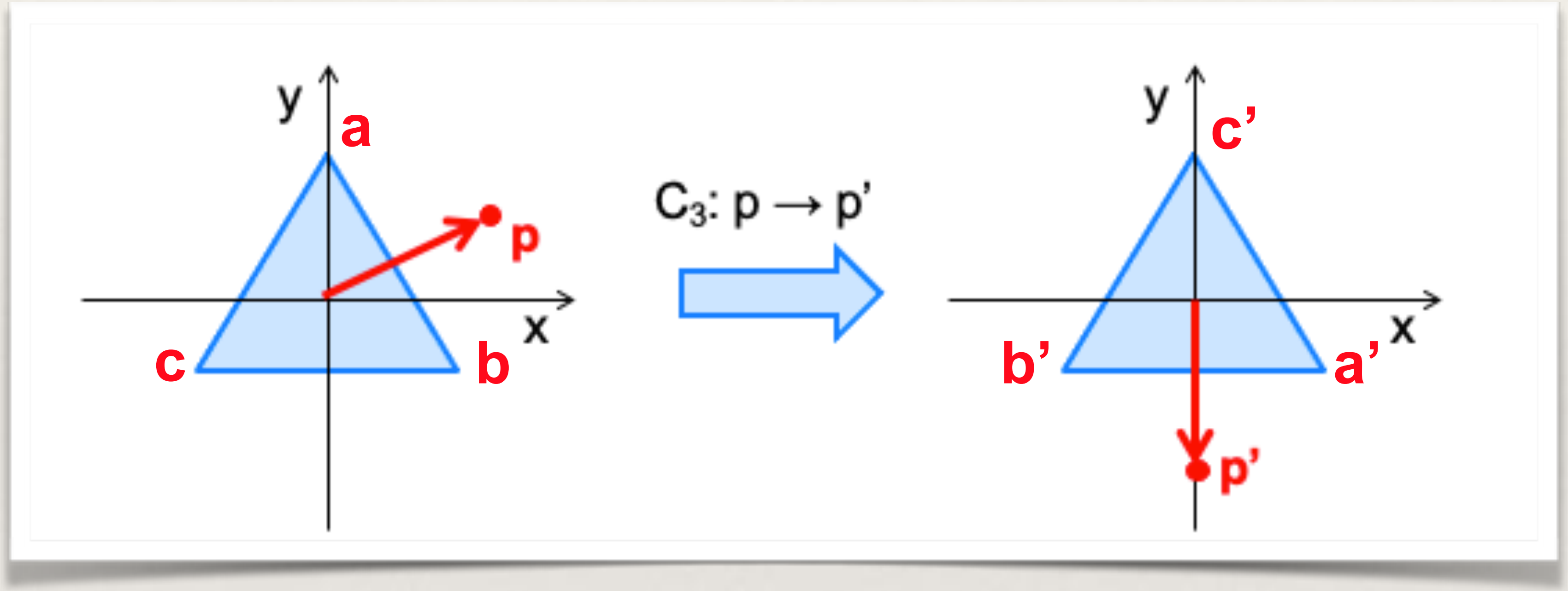
Hermann Weyl, 1885 - 1955

Given a spatial configuration $\mathfrak{F}$, those **automorphisms of space** which leave $\mathfrak{F}$ unchanged **form a group Γ**, and this group describes exactly the symmetry possessed by $\mathfrak{F}$.



Automorphisms of Euclidean space

A geometrical object has **a symmetry** if there is an **automorphism** in Euclidean space, that is, a function T: $R^3 \rightarrow R^3$, that maps the object onto itself:

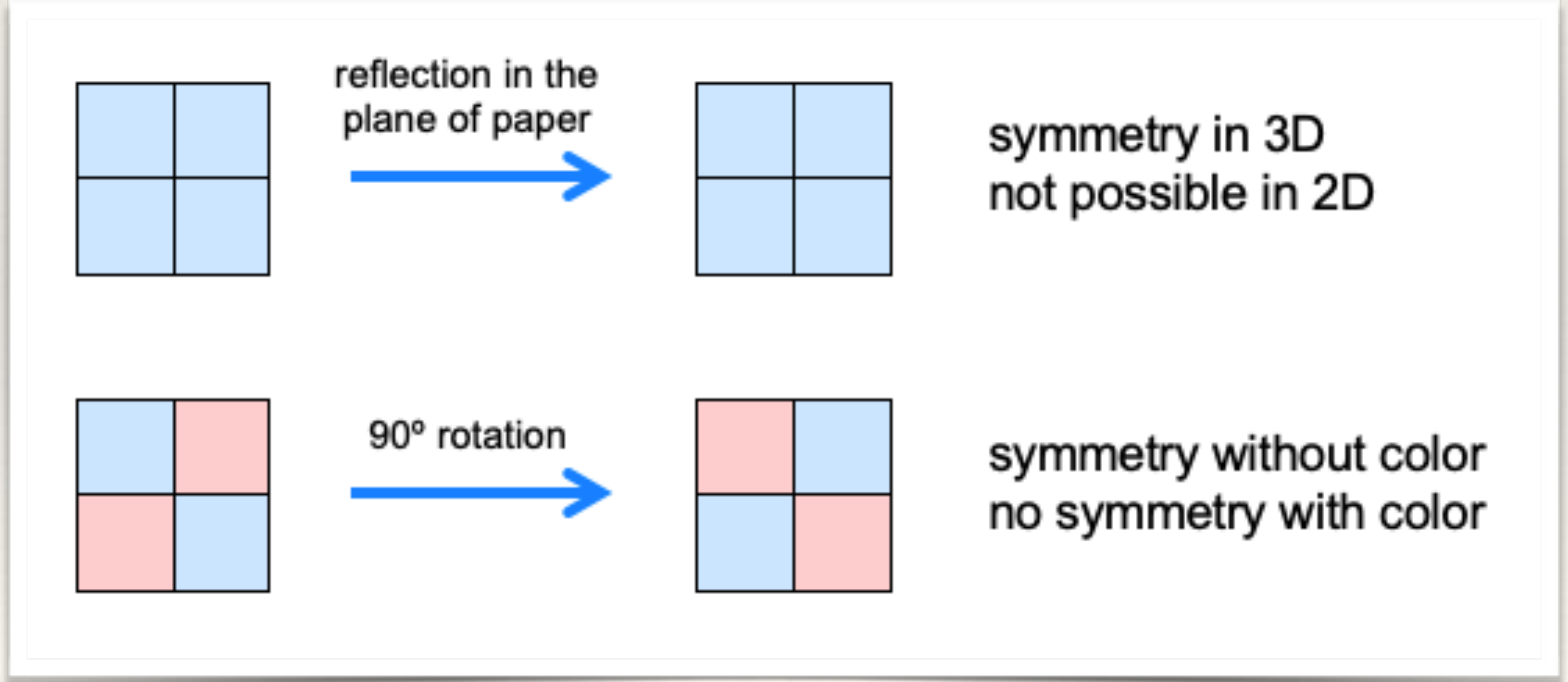


T: $R^3 \rightarrow R^3$ is a function for the **whole space**, not only for the points in the object.

To map the object onto itself, T must be an **isometry**, that is, a **distance preserving automorphism**.

Types of symmetry

The types of symmetries that are possible for an object depend on the set of **available geometric transformations** and which **object properties** should remain unchanged after a transformation



Algebra (High school version)

Branch of mathematics concentrating in solving equations:

Solve $5(x-3)=4x+9-x$

Simplify each side of the equation	$5(x-3)=4x+9-x$ $5x-15=3x+9$
Add the opposite of -15 to both sides.	$5x-15+15=3x+9+15$
Simplify.	$5x=3x+24$
Add the opposite of 3x to both sides.	$5x-3x=3x+24-3x$
Simplify.	$2x=24$
Multiply both sides by the reciprocal of 2.	$\frac{1}{2}\cdot 2x=\frac{1}{2}\cdot 24$
Simplify.	$x=12$

Abstract (modern) algebra

Branch of mathematics seeking to reveal the **basic principles** which apply equally to all known and possible "algebras"

Algebraic structures

Arbitrary set of **objects** (numbers, matrices, functions, permutations, symmetry operations, …) and certain **operations** defined between them (addition, multiplication, concatenation, …)

Example:

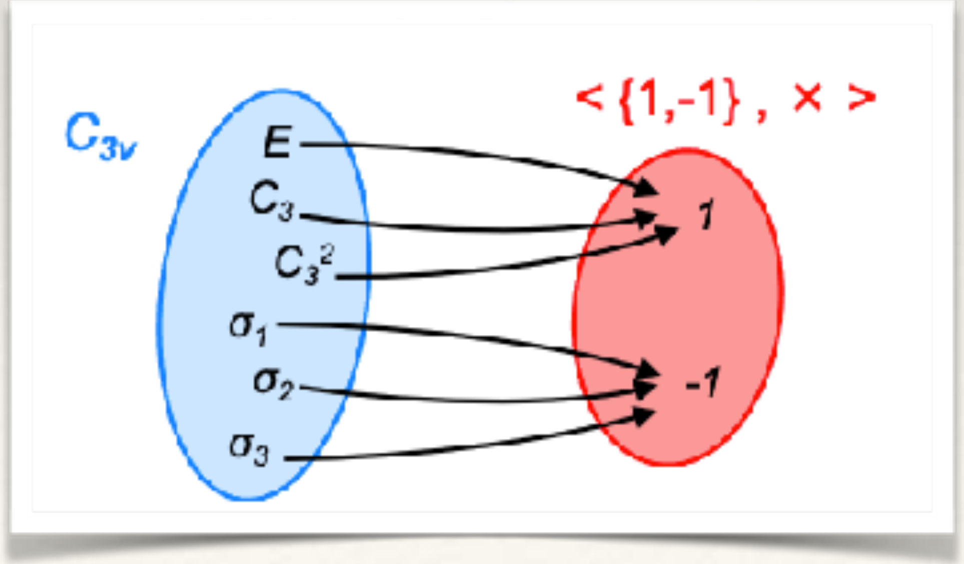
Groups, vector spaces, modules, …

Morphisms

Structure-preserving maps from one algebraic structure to another one of the same type.

Example:

Homomorphism between groups



Operations

An operation $*$ on a set A is a rule which assigns to **each ordered pair** (a,b) of A **exactly one element in A**: c= a $*$ b

$\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$

set of integer numbers

a = -3
b = 5

Sum

(-3) + 5 = 2

Multiplication

(-3) x 5 = -15

M = set of 2x2 matrices withreal coeficients

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

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

Matrix sum

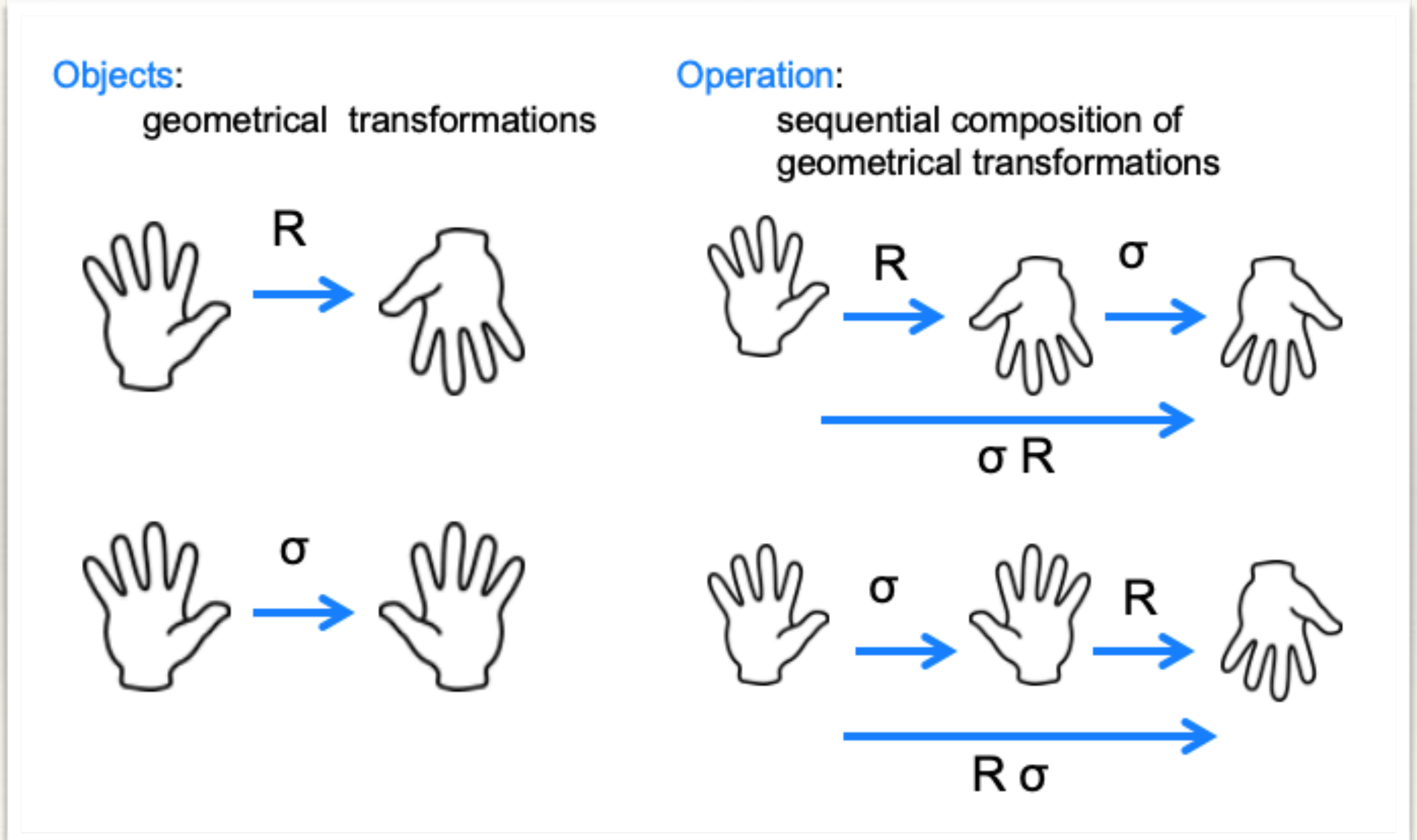
$A+B = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$

Matrix multiplication

$AB = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}$

$BA = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$

Operations between geometric transformations



Basic properties of proper operations

- The operation $a * b$ must be **defined for all ordered pairs** $a , b \in A$

  Division in $\mathbb{R}$ is not a proper operation since $a \div 0$ is not defined

- The result $a * b$ of an operation must be **uniquely defined**

- **Closure condition**: if $a,b \in A$ then $a * b$ must be an element of A

  Division in $\mathbb{Z}$ is not a proper operation since $a \div b$ is not always in $\mathbb{Z}$

Associativity

An operation is a rule to combine two elements, so, if we want to combine three elements $a, b, c \in A$ we have two choices:

$$a * (b * c) \text{ or } (a * b) * c$$

The operation is said to be **associative** if

$$a * (b * c) = (a * b) * c \quad \text{for any } a, b, c \in A$$

All operations considered here will be associative:

sum and multiplication of numbers / matrices
sequential composition of geometric transformations / permutations

Commutativity

An operation is said to be **commutative** if:

$$a * b = b * a$$

for any a,b ∈ A

Multiplication in $\mathbb{Z}$ is commutative

$3 \times 7 = 21$

$7 \times 3 = 21$

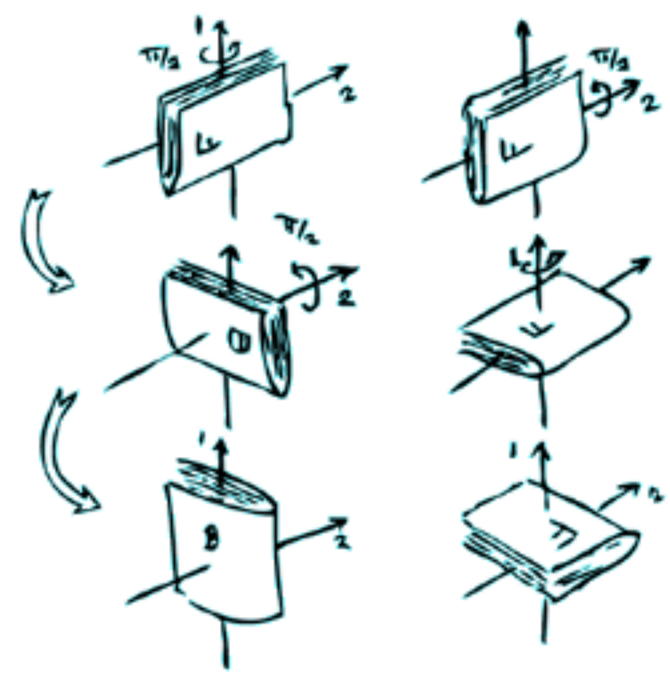
Matrix multiplication is not commutative

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

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

$$AB = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} = BA$$

Rotations in space do not commute



Neutral element

If there is an element e ∈ A such that:

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in A$$

e is called the **neutral element** (or identity) of A with respect to *

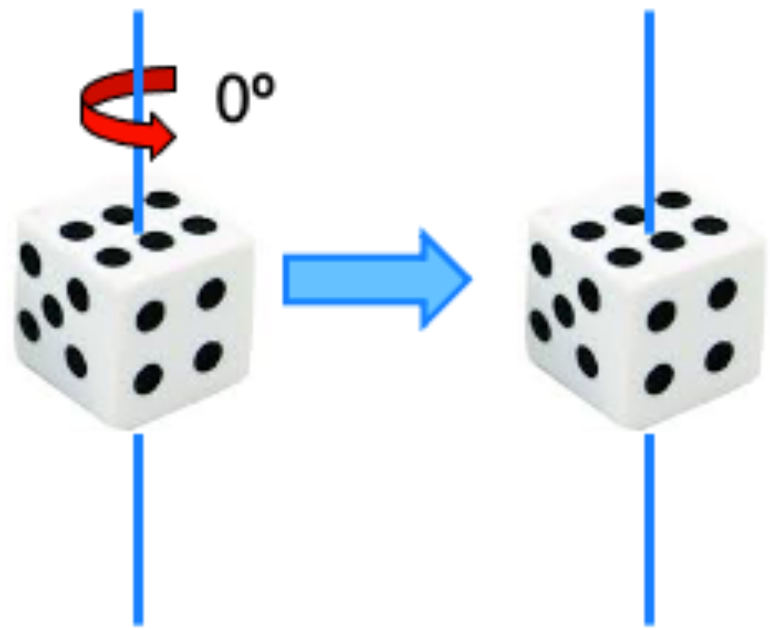
neutral element for multiplication
of in the set of 2x2 matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{AI = IA = A}$$

0 neutral element for addition
of real numbers

1 neutral element for multiplication
of real numbers

neutral element for rotations
around a given axis

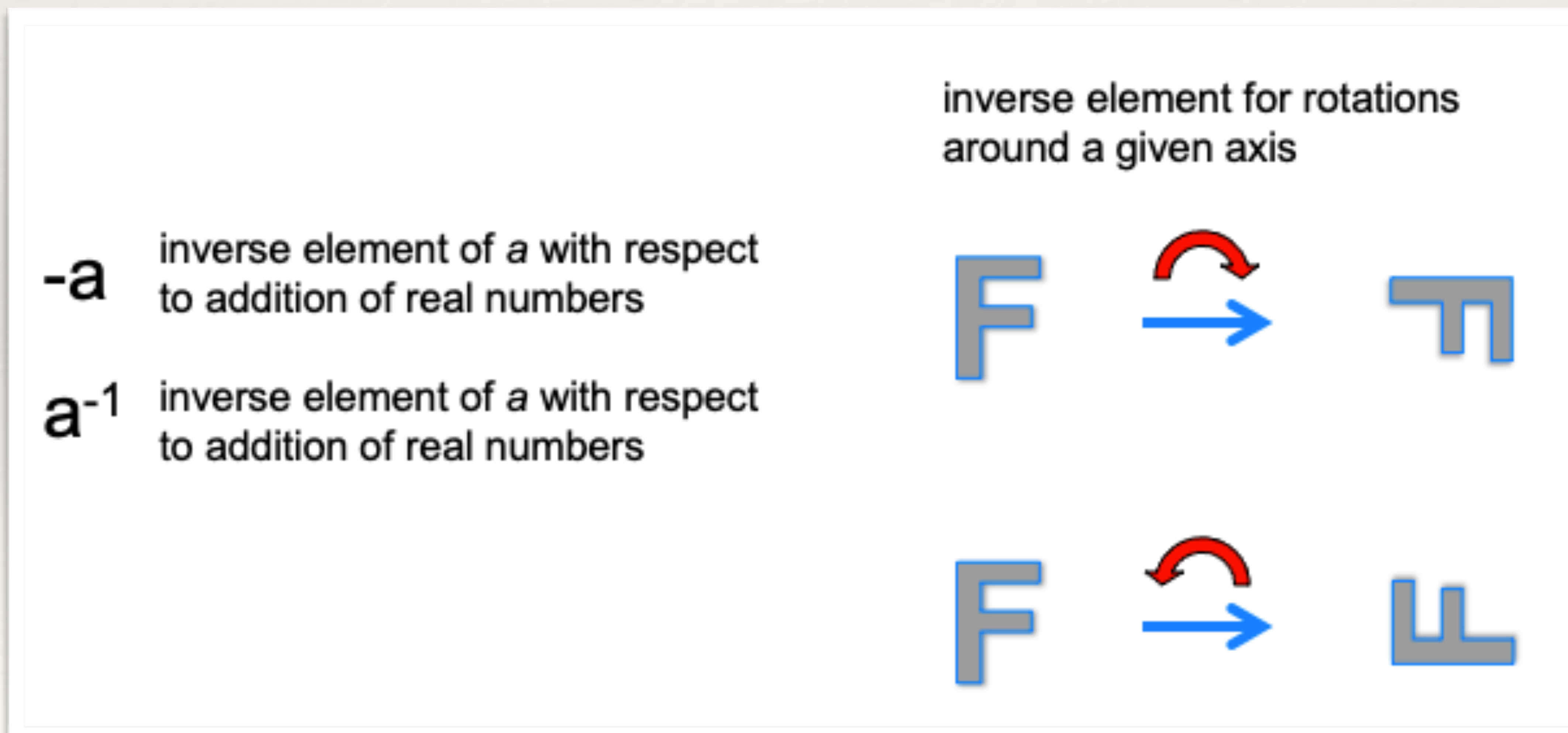


Inverse elements

If there is an element x ∈ A such that:

$$x * a = e \quad \text{and} \quad a * x = e$$

then x is called the **inverse** of a with respect to *



Groups

A **group** <G, $*$ > is a **set G** with an **operation** $*$ satisfying:

1) G is **closed** with respect to the **associative** operation $*$
2) There is a **neutral element** e with respect to $*$ in G
3) For each a $\in$ G there is also its **inverse** a^{-1} with respect to $*$ in G

The number of elements in G is called the **order of the group**, h_G or $|G|$

If h_G is finite we speak of **finite groups**, if it is infinite, then G is an **infinite group**

Commutativity is not included in the definition, but we may have commutative or **Abelian groups** which have this extra property

Infinite Groups

Some examples of infinite groups

$\mathbb{Z}=\{\ldots,-2,-1,0,1,2,\ldots\}$	$\langle \mathbb{Z},+\rangle$	The additive group of the integers
$GL_n(R)$	The general linear group over the real numbers of order n	The set of *n* x *n* invertible matrices of real numbers with the operation of ordinary matrix multiplication
O(3)	The orthogonal group	The set of *3* x *3* orthogonal matrices ($R^TR = I$) and the operation of ordinary matrix multiplication
SO(3)	The special orthogonal group	The set of *3* x *3* orthogonal matrices ($R^TR = I$) with det(R) = 1 and the operation of ordinary matrix multiplication

Finite Groups

Some examples of finite groups

$G = \{-i, i, -1, 1\}$ with ordinary multiplication of complex numbers

$\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ with addition modulo 6

Permutations of 3 elements with the sequential composition of permutations

S_3: the symmetric group of 3 elements

$$p_0 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix} \quad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix} \quad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix}$$

$$[p_1 \circ p_2](1) = p_1(p_2(1)) = p_1(3) = 2$$
$$[p_1 \circ p_2](2) = p_1(p_2(2)) = p_1(1) = 1$$
$$[p_1 \circ p_2](3) = p_1(p_2(3)) = p_1(2) = 3$$

$$p_1 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix} = p_3$$

Multiplication table

Table containing the result of the operation for all possible ordered pairs of the set. The multiplication table highlights the structure of the group.

$G = \{-i, i, -1, 1\}$

with ordinary multiplication of complex numbers

<G,*>	1	i	-i	-1
1	1	i	-i	-1
i	i	-1	1	-i
-i	-i	1	-1	i
-1	-1	-i	i	1

a

b

a*b

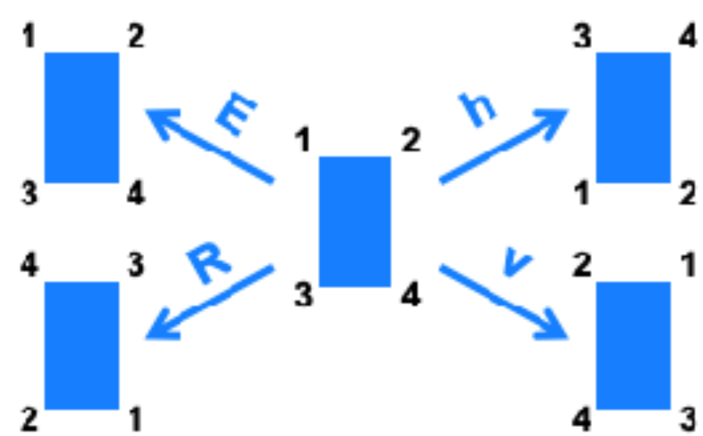
V	E	R	v	h
E	E	R	v	h
R	R	E	h	v
v	v	h	E	R
h	h	v	R	E

T

S

(TS)O = T(SO)

V: symmetry operations of a rectangle



All elements of G must appear in each row / column.

If the table has reflection symmetry across the diagonal, then G is Abelian.

Different groups with the same table have the same structure.

Subgroups

If G is a group and S a nonempty subset of G such that:

- S is closed under multiplication
- S is closed with respect to inverses

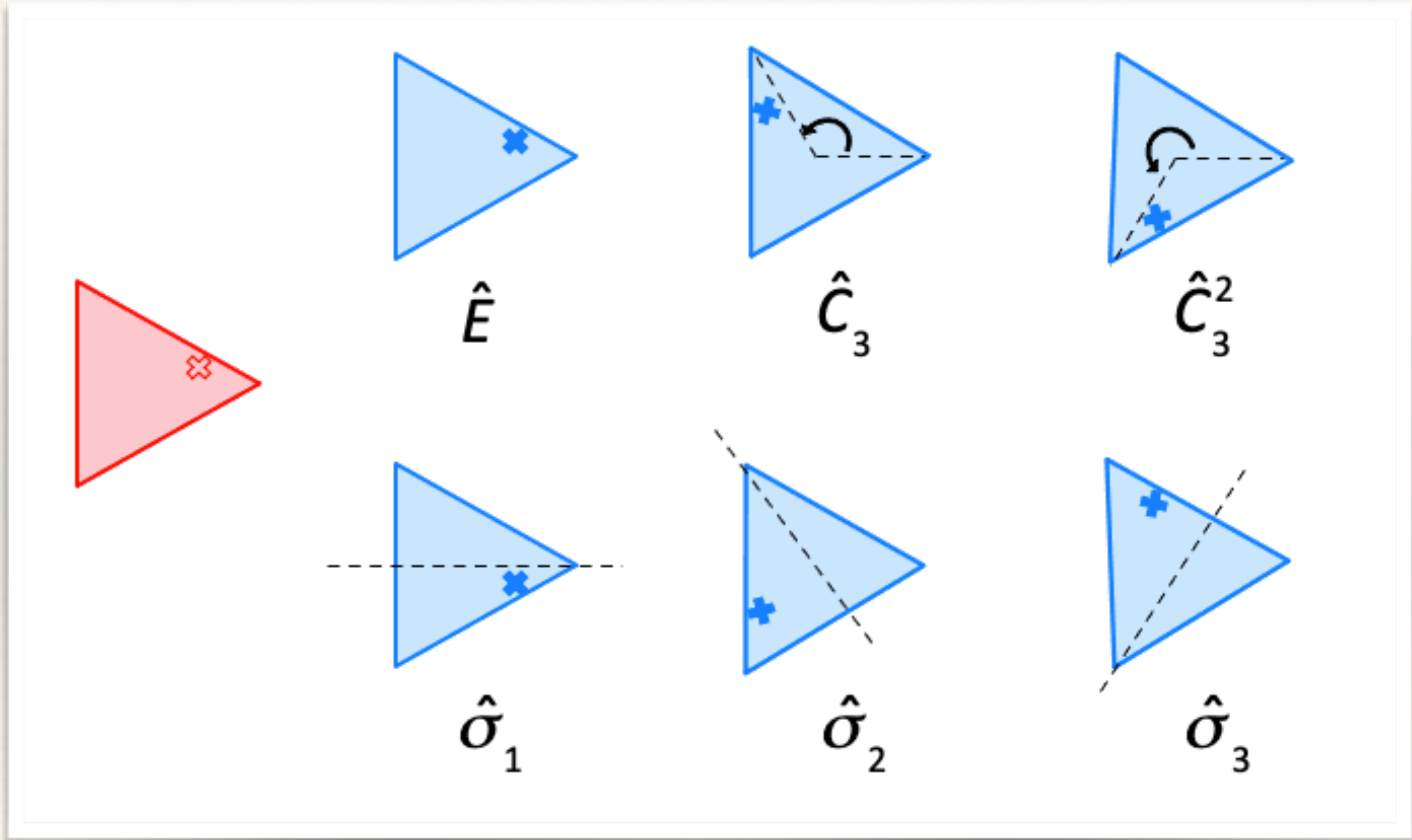
Then S is itself a group and it is called a **subgroup** of G written as $S \subset G$.

Every group G has two **trivial subgroups**: the group G itself and {e}. All other subgroups are called **proper subgroups**.

All subgroups S of a group G share, at least, the identity e

The symmetry group of an equilateral triangle

An equilateral triangle has the six symmetry operations of the C_{3v} group



In 3D, the plane containing the triangle is a reflection plane, the C_3 axis becomes also a S_3 axis, and there are 3 additional C_2 rotation axes in the plane. The full symmetry group in 3D is D_{3h} with h =12.

The structure of C_{3v}

	E	**C_3**	**C_3^2**	**σ_1**	**σ_2**	**σ_3**
E	E	C_3	C_3^2	σ_1	σ_2	σ_3
C_3	C_3	C_3^2	E	σ_3	σ_1	σ_2
C_3^2	C_3^2	E	C_3	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	E	C_3	C_3^2
σ_2	σ_2	σ_3	σ_1	C_3^2	E	C_3
σ_3	σ_3	σ_1	σ_2	C_3	C_3^2	E

Proper subgroups

$C_3 = \{ E , C_3 , C_3^2 \}$

$C_s = \{ E , \sigma_1 \}$

$C_s' = \{ E , \sigma_2 \}$

$C_s'' = \{ E , \sigma_3 \}$

all 4 proper subgroups are cyclic and abelian

C_{3v} is a non-commutative group

e.g. $C_3\sigma_1 = \sigma_3$

$\sigma_1 C_3 = \sigma_2$

C_3 and σ_1 are a set of generators for C_{3v} :

$$C_3^2 = C_3 C_3$$

$$E = C_3 C_3 C_3 = \sigma_1\sigma_1$$

$$\sigma_2 = C_3^2 \sigma_1 = C_3 C_3 \sigma_1$$

$$\sigma_3 = C_3 \sigma_1$$

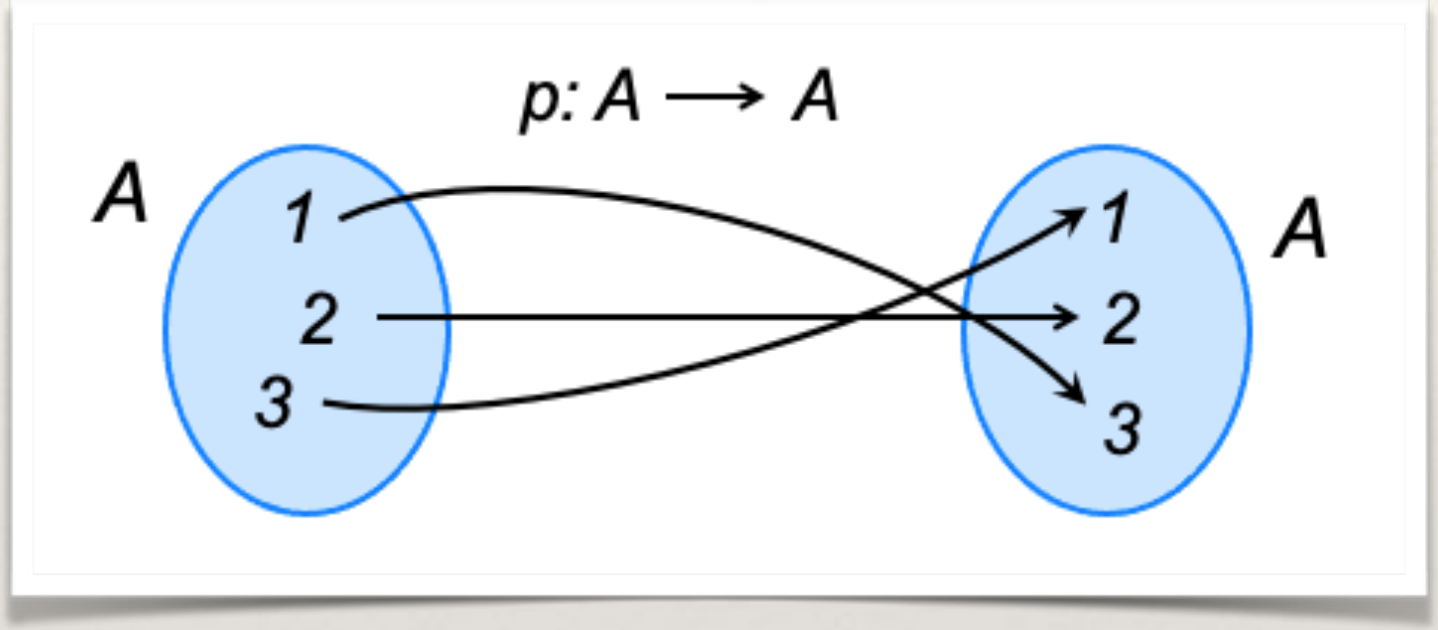
C_{3v} as a direct product:

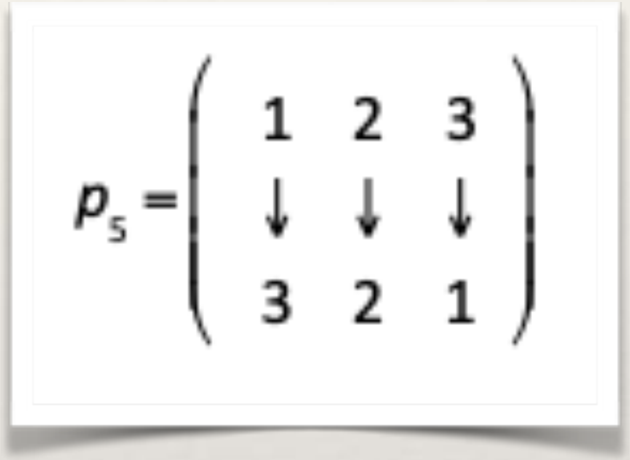
$$C_{3v} = C_3 \otimes C_s$$

where (g,h) = gh

Permutations of a set

A permutation of a set A is a **bijective** function from A to A:





The composition of two permutations $p_2 \circ p_1$ is also a permutation. Two permutations are equal if and only if $p_1(x) = p_2(x)$ for every $x \in A$.

Symmetric group S_n

The set of all permutations of a set A with *n* elements together with the operation $p_r \circ p_s$ of permutation composition, is a group S_n of order n! called the symmetric group on n elements.

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Identity: $\varepsilon \circ p_n = p_n \circ \varepsilon = p_n$

Inverse: $p_n^{-1} \circ p_n = p_n \circ p_n^{-1} = \varepsilon$

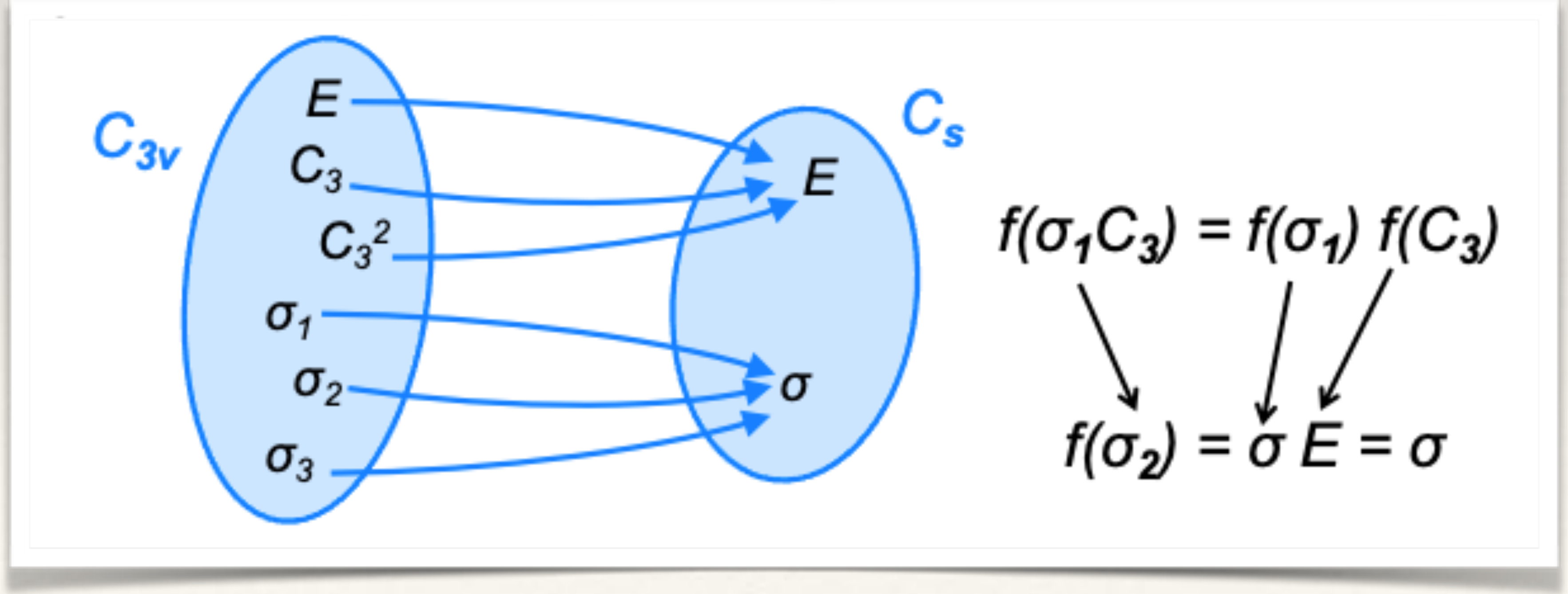
S_3	ε	p_1	p_2	p_3	p_4	p_5
ε	ε	p_1	p_2	p_3	p_4	p_5
p_1	p_1	ε	p_3	p_2	p_5	p_4
p_2	p_2	p_5	p_4	p_1	ε	p_3
p_3	p_3	p_4	p_5	ε	p_1	p_2
p_4	p_4	p_3	ε	p_5	p_2	p_1
p_5	p_5	p_2	p_1	p_4	p_3	ε

Group homomorphisms

If G and H are groups, a homomorphism from G to H is a function f: G → H such that for any two elements a, b ∈ G

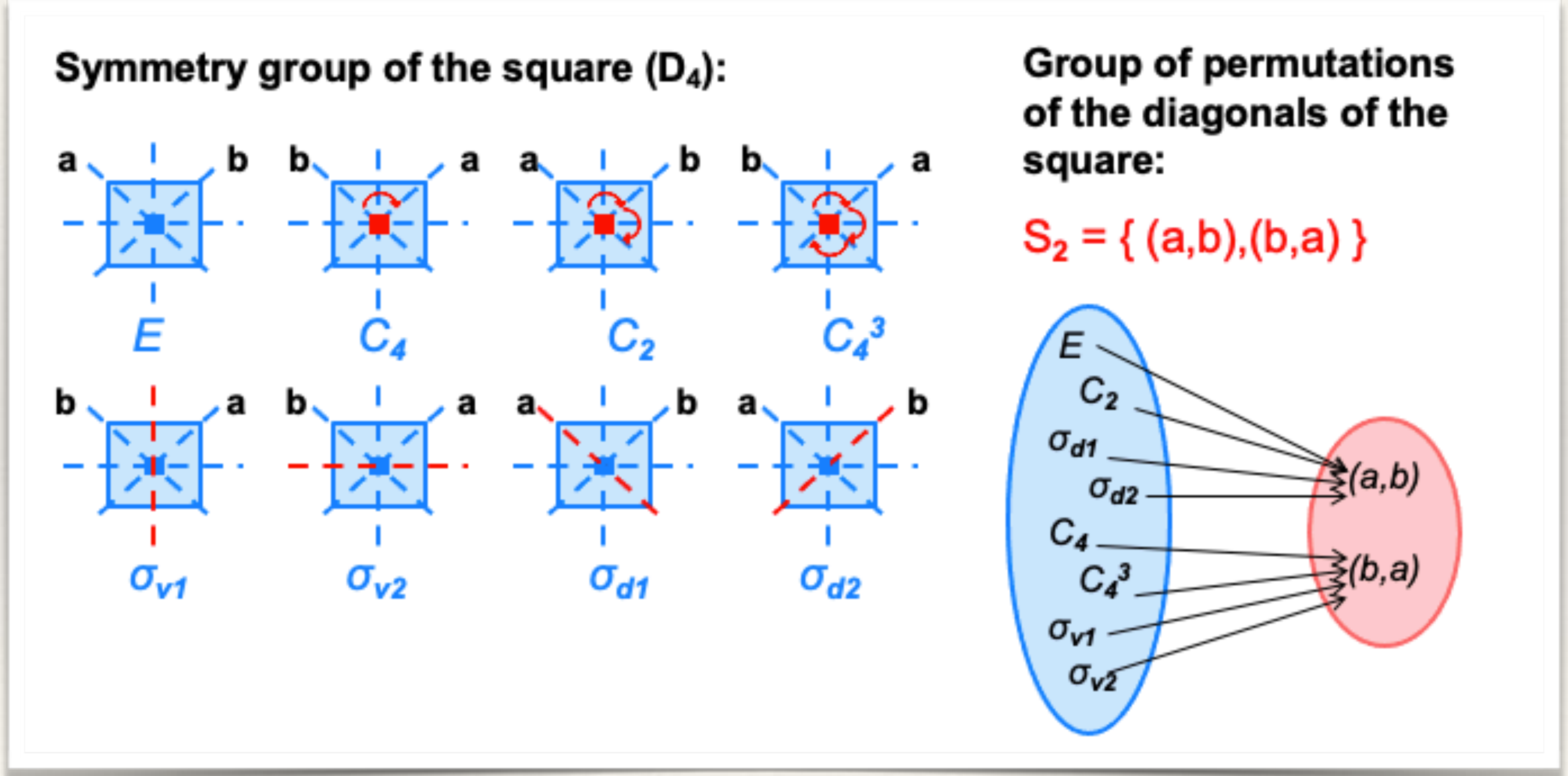
$$f(ab) = f(a)\, f(b)$$

If there exists an homomorphism from G onto H, we say H is an homomorphic image of G. Homomorphic images preserve some features of the structure of the original group.



Why are homomorphisms interesting

Homomorphisms are one of the key aspects in group theory since they allow us to discard aspects of a group while keeping those of interest for a given problem



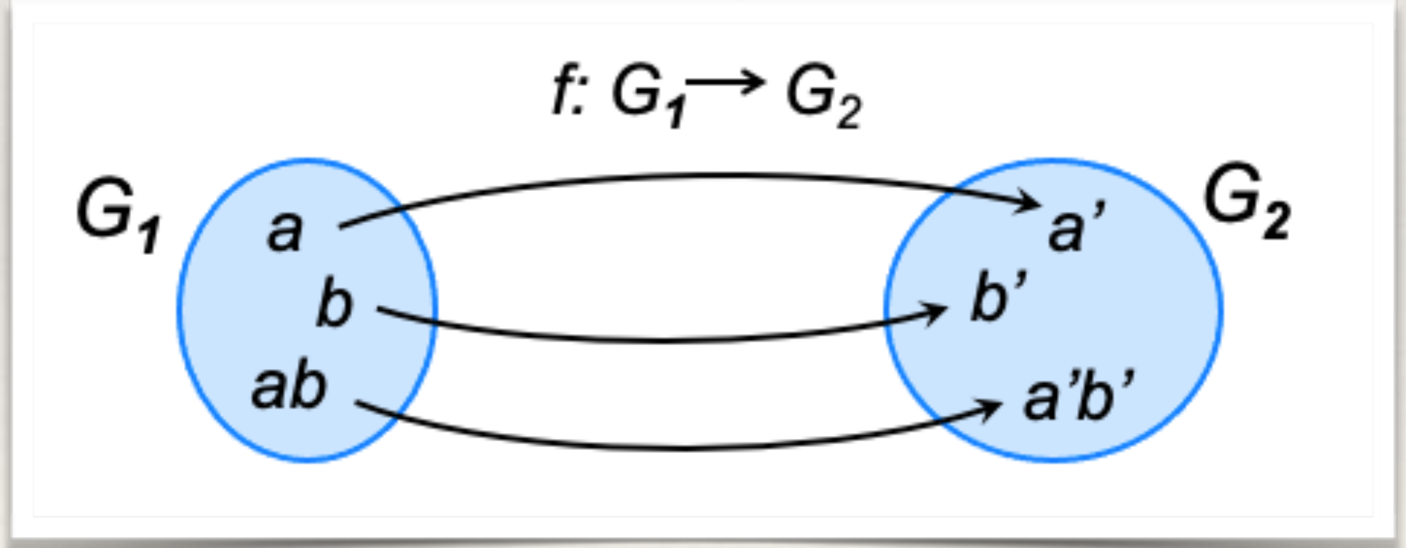
S_2 is a homomorphic image of D_4 where only the information about the motions of the diagonals of the square under the operations of D_4 are retained.

Group isomorphisms

Let G_1 and G_2 be groups. A bijective function $f: G_1 \to G_2$ such that for any two elements $a, b \in G_1$

$$f(ab) = f(a)\, f(b)$$

is said to be an isomorphism from G_1 to G_2 and the two groups are said to be isomorphic: $G_1 \cong G_2$.



All isomorphic groups share the same structure, and from an algebraic point of view they are all representatives of the same abstract group.

The cyclic group of 3 elements

There is only one possible multiplication table for a group with 3 elements, so that all order 3 groups are isomorphic between them.

$\mathbb{Z}_2 = \{0,1,2\}$ with addition modulo 2

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $B = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$ $C = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$

	E	B	C
A	A	B	C
B	B	C	A
C	C	A	B

$Z_3 = \{a, a^2, a^3 = e\}$

Z_3	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

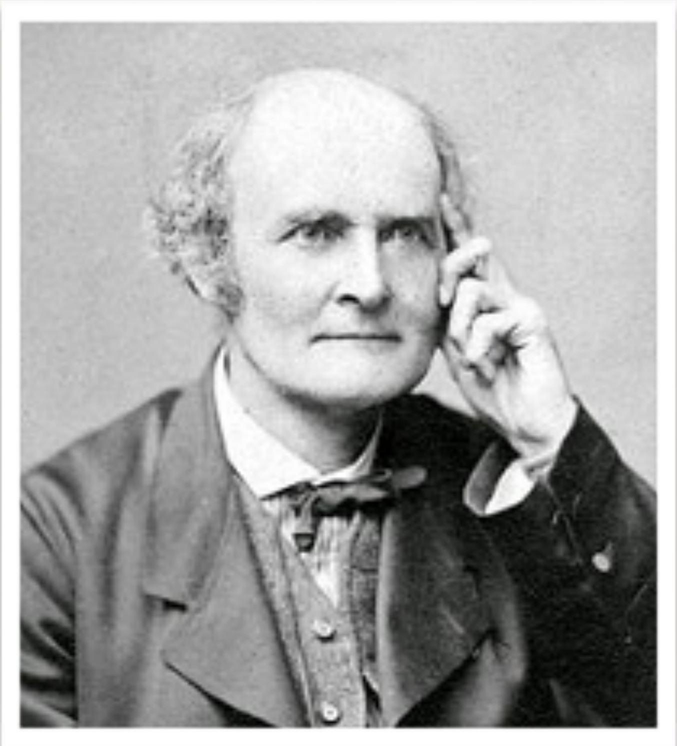
All three groups have exactly the same structure: they are isomporphic to Z_3

	E	C_3	C_3^2
E	E	C_3	C_3^2
C_3	C_3	C_3^2	E
C_3^2	C_3^2	E	C_3

$\hat{E}$ $\hat{C}_3$ $\hat{C}_3^2$

Cayley's Theorem

Every group is isomorphic to a group of permutations.



Arthur Cayley (1821-1895)

Using the concept of isomorphism it has been possible to classify finite groups into a few families and to find out the number of different (non isomorphic) finite groups of a given order

Order n	# of groups	Abelian	Non-Abelian
1	1	1	0
2	1	1	0
3	1	1	0
4	2	2	0
5	1	1	0
6	2	1	1
7	1	1	0
8	5	3	2
9	2	2	0
10	2	1	1
11	1	1	0
12	5	2	3

Abstract 4-element groups

There are only two fundamentally different groups with 4 elements.

V: Klein four-group

$<a,b \mid a^2 = b^2 = (ab)^2 = e>$

2D: symmetry group of a rectangle or a rhombus $\{ E, C_2, \sigma_x, \sigma_y \}$

3D: $C_{2v} = \{ E, C_2, \sigma_v, \sigma'_v \}$
$C_{2h} = \{ E, C_2, \sigma_h, i \}$
$D_2 = \{ E, C_{2(x)}, C_{2(y)}, C_{2(z)} \}$

V	**e**	**a**	**b**	**ab**
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
c	ab	b	a	e

Z_4	**e**	**a**	**a^2**	**a^3**
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

Z_4: Cyclic group of order 4

$<a \mid a^4 = e>$

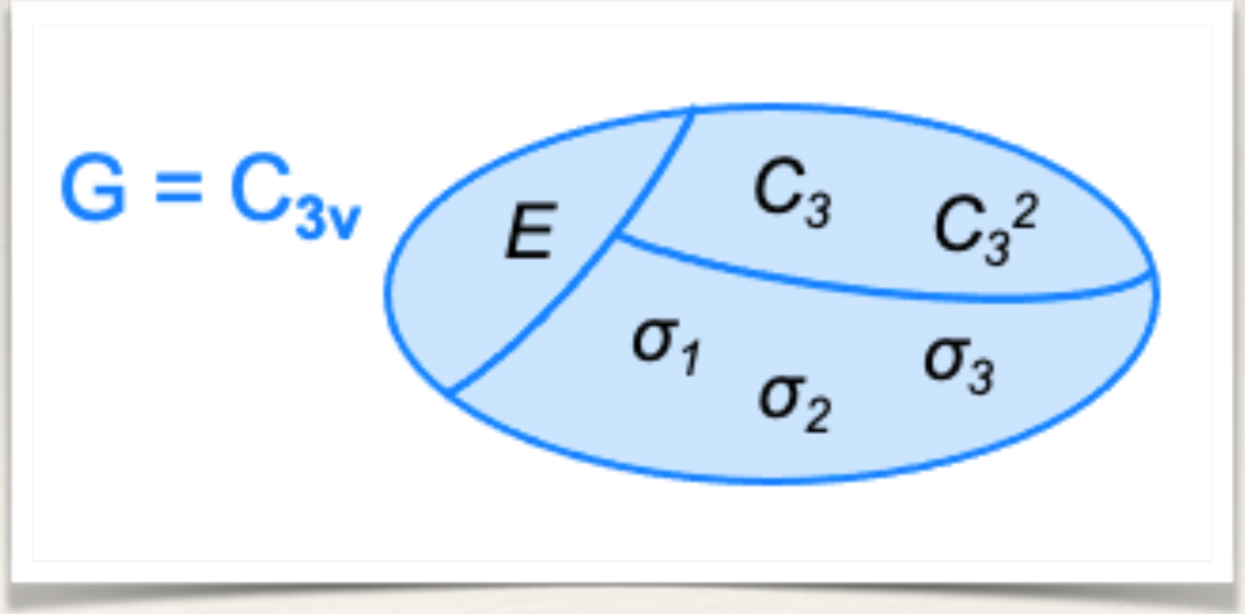
Symmetry group of fourfold rotations

$C_4 = \{ E, C_4, C_4^2 = C_2, C_4^3 \}$

Conjugate elements

For $a \in G$, any element $b = xax^{-1}$ where $x \in G$ is said to be **conjugate** of a.

The relation $a \sim b$ (a is conjugate of b) **partitions** G into **conjugacy classes** (the conjugacy class of a is the set of all elements $b = xax^{-1}$)



Subgroups do not partition a group (they must share, at least, the identity E)

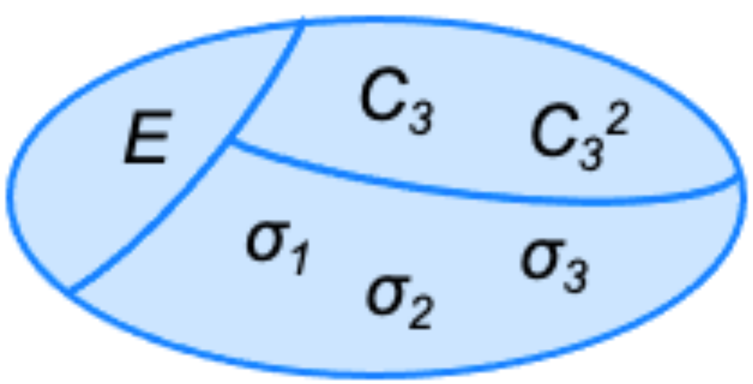
Conjugacy classes contain "similar" elements

Normal subgroups

Let N be a subgroup of a group G. N is called a normal subgroup of G if it is closed with respect to conjugates, that is, if

$$\forall a \in N \text{ and } \forall x \in G \text{ then } xax^{-1} \in N$$

Conjugacy classes of C_{3v}



$C_3 = \{E, C_3, C_3^2\}$ is a normal subgroup of C_{3v} since it is closed with respect to conjugates

$C_s(1) = \{ E, \sigma_1 \}$ is not a normal subgroup since $\sigma_1 \sim \sigma_2$ and $\sigma_1 \sim \sigma_3$

Any group G has, at least, two trivial normal subgroups,{E} and G itself.

The fundamental homomorphism theorem

The FHT states that all homomorphic images of a group G are isomorphic to a quotient group G/N of G.

Since there are only three normal subgroups in C_{3v} we can have, up to isomorphism, only three different homomorphic images of C_{3v}.