EPJ Web of Conferences **22**, 00004 (2012)
DOI: 10.1051/epjconf/20122200004

Introduction to group theory

B. Canals[1] and H. Schober[2]

[1] *Institut Néel, CNRS and University Joseph Fourier, BP. 166, 25 avenue des Martyrs, 38042 Grenoble Cedex 9, France*
[2] *Institut Laue-Langevin, BP. 156, 38042 Grenoble Cedex 9, France, and Université Joseph Fourier, UFR de Physique, 38041 Grenoble Cedex 9, France*

Abstract. This chapter is a concise mathematical introduction into the algebra of groups. It is build up in the way that definitions are followed by propositions and proofs. The concepts and the terminology introduced here will serve as a basis for the following chapters that deal with group theory in the stricter sense and its application to problems in physics. The mathematical prerequisites are at the bachelor level.[1]

1. GROUP STRUCTURE

An algebraic structure is a set of elements (the carrier of the structure) with an operation (equally denoted application) that matches any two members of the set uniquely onto a third member. The specificity of an algebraic structure is given by the axioms that it satisfies. One of the most basic algebraic structures is the group.

(1.1) Definition.
A **group** is a couple (G, μ) where:
1) G is a set
2) μ is an application, $\mu : G \times G \longmapsto G$
3) $\forall a, b, c \in G$, the relation $\mu(a, \mu(b, c)) = \mu(\mu(a, b), c)$ is fullfilled
4) $\exists e \in G$ such that $\forall a \in G$, the relation $\mu(e, a) = \mu(a, e) = a$ is fullfilled
5) $\forall a \in G, \exists b \in G$ such that $\mu(a, b) = \mu(b, a) = e$.

Thus, apart from closure (axiom 2), which is applicable to any algebraic structure, a group is characterized by the properties of associativity (axiom 3), identity (axiom 4) and invertibility (axiom 5).

From the group axioms it can be derived that both the identity and the inverse elements are unique. Formally:

(1.1) Proposition.
If (G, μ) is a group, then
a) the element e whose existence is guaranteed by axiom 4, is unique.
b) $\forall a \in G$, b the inverse of a in G, the existence of which is guaranteed by axiom 5, is unique.

---

[1] Supplementary material for illustration can be found in the presentation slides of B. Canals (http://www.ill.eu/news-events/past-events/2009/ecole-theorie-des-groupes/transparents-cours-td-tp/). The reader who would like to learn more about the mathematical foundation of group theory is referred to the literature [1, 2].

Proof.
a) Let e_1 and e_2 be two elements of (G, μ) satisfying axiom 4.
e_1 satisfies (4), so $\mu(e_1, e_2) = e_2$.
e_2 satisfies (4), so $\mu(e_1, e_2) = e_1$.
Therefore $e_1 = \mu(e_1, e_2) = e_2$.

b) Given $a \in G$ and b_1, b_2 two elements of (G, μ) satisfying axiom 5.
Then $\mu(a, b_1) = \mu(b_1, a) = e$ and $\mu(a, b_2) = \mu(b_2, a) = e$.
We have $\mu(b_1, \mu(a, b_2)) = \mu(b_1, e) = b_1$.
Because the μ law is associative (3), $\mu(b_1, \mu(a, b_2)) = \mu(\mu(b_1, a), b_2) = \mu(e, b_2) = b_2$, which means that $b_1 = b_2$. □

Terminology.
The unique element $e \in (G, \mu)$ fulfilling condition (4) is called the neutral element of (G, μ).
For all $a \in (G, \mu)$, the unique element b satisfying $\mu(a, b) = \mu(b, a) = e$ is called the inverse of a in (G, μ).
The component μ of (G, μ) is called the law of (G, μ) or sometimes, the inner law[2].

Instead of talking of the group (G, μ), one often talks of the G group and its inner law μ. For instance, one will talk of the $\mathbb{Z}$ group and its additive $+$ law, of the $\mathbb{Q}_*$ group and its mutiplicative $\times$ law, or of the $SL_2(\mathbb{Z})$ group[3] and its multiplicative $\cdot$ law.

Examples of groups
Many mathematical structures that are familiar to us satisfy group axioms. This is e.g. the case for the set of integer numbers with the addition as the group application $(\mathbb{Z}, +)$.
- $(G, \mu) = (\mathbb{Z}, \alpha) = (\{\text{integers}\}, \alpha)$ where

$$\alpha : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(m, n) \longmapsto m + n$$

Are the group axioms satisfied?
(1) and (2) are satisfied as the addition of two integer numbers gives an integer number.
So is (3) because addition is associative.
(4) : is there an $e \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}, \alpha(e, a) = \alpha(a, e) = a$? Yes, we have $e = 0$.
(5) : $\forall a \in \mathbb{Z}$, is there a $b \in \mathbb{Z}$ such that $\alpha(a, b) = \alpha(b, a) = e = 0$? Yes, we have $b = -a$.
Therefore $(\mathbb{Z}, \alpha)$ is a group.

Remark.
$(\mathbb{Q}, \times)$ with $\mathbb{Q}$ the set of rationals and $\times$ the multiplication is not a group because (5) is not fulfilled for $a = 0$.

A particularly useful property of groups is the so-called simplification rule.

---

[2] The word "inner" comes from the fact that the two elements a and b taken to form $\mu(a, b)$ are in the group; this notion is, therefore, related to the input, not the output. Conversely, one will talk of an *external* law when dealing with the multiplication of an element of a vector space with a scalar. The fact that $\mu(a, b) \in G$ is a closure condition; one sometimes states that (G, μ) is closed.

[3] The special linear group $SL_2(\mathbb{Z})$ or $SL(2, \mathbb{Z})$ is the group of all integer 2×2 matrices with determinant one.

(1.2) Proposition.
Let G be a group. Then $\forall a, b, c \in G$,

$$ab = ac \quad \Rightarrow \quad b = c \qquad \text{(left simplification by } a\text{)}$$
$$ba = ca \quad \Rightarrow \quad b = c \qquad \text{(right simplification by } a\text{)}$$

Proof.
$ab = ac$; we left multiply by a^{-1}

$$a^{-1}(ab) = a^{-1}(ac)$$
$$(a^{-1}a)b = (a^{-1}a)c \quad \text{associativity}$$
$$eb = ec$$
$$b = c$$

We, therefore, have $b = c$. □

As we will see in the later chapters groups are the mathematical structures that allow to capture the notion of symmetry. Talking about symmetry always presupposes that the objects under consideration can be operated upon. In other terms, it has to be possible to produce images and to compare those images with the original. The most interesting operations in terms of symmetry are those that match an object onto itself, the so-called symmetry operations. A common example of physical operations are rotations in space. Two physical operations can be combined into a third one by executing them consecutively. Physical operations thus form a closed set with an application (inner law of combination). This set contains the identity and the inverse elements (the operations that produce the originals from the images). As the inner law is in general associative, physical operations possess the structure of a group.[4]

A particularly important class of groups are the so-called commutative or abelian groups.

(1.2) Definition.
The group (G, μ) is **abelian** or **commutative** if $\forall a, b \in G, \mu(a, b) = \mu(b, a)$.

Terminology.
If (G, μ) is commutative, one often uses the infixed $+$ notation for the inner law, often called the additive notation.
Otherwise, i.e. when the group is not commutative, one almost always uses the multiplicative notation, $(a \times b, a \cdot b, ab)$.

Example.
The vector product is a non commutative group:

$$\mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$
$$\vec{a} \times \vec{b} \longmapsto \vec{c}$$

Attention: $(\mathbb{Q}_*, \times)$ is the multiplicative group of non zero rationals and is commutative.

[4] We will see in the following that the groups possess a life of their own, i.e. that they can be dissociated from the objects that they act upon. In other words, the type of these physical operations does not matter. As soon as one can identify a group structure, it is possible to apply all the generic tools of group theory, and once all properties of the formal algebraic structure are derived, it is then possible to interpret those properties as physical properties.

Terminology.
If the law of a group is a multiplicative law (non commutative), then, if $a \in G$ and if $n \in \mathbb{N}$, one notes

$$a^n = \underbrace{a \cdot a \cdot \ \ldots \ \cdot a}_{n \text{ times}}.$$

In particular, $a^1 = a$; $a^m a^n = a^{m+n}$ and a^0 is the empty product = neutral element = e and consequently, $a^0 \cdot a^m = a^{0+m} = a^m$.

If a^{-1} is the inverse of a, then $a^{-1} \cdot a^1 = a^0 = e$ and more generally,

$$a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdot \ \ldots \ \cdot a^{-1}}_{n \text{ times}} = \left(a^{-1}\right)^n$$

This implies that the exponent law applies $\forall m, n \in \mathbb{Z}$.

If the law of a group is an additive law (commutative) and if $n \in \mathbb{N}$, one generally uses

$$n \cdot a = \underbrace{a + a + \ \ldots \ + a}_{n \text{ times}}$$

$0 \cdot a = e$ is most often noted by 0.

$-a$ = opposite of a = inverse of a with respect to $+$ and of course,

$$-na = n(-a) = \underbrace{(-a) + (-a) + \ \ldots \ + (-a)}_{n \text{ times}}.$$

2. SUBGROUPS AND PRODUCT GROUP

Any group may contain a subset of elements that fulfills all the conditions of a group.
To form a subgroup of the group G a set H has to comply with the following requirements:
1) The identity element (as it is unique) has to belong to H.
2) The set H is closed under the law that G induces in H.
3) Every element of H has its inverse element in H.

Formally:

(2.1) Definition.
Let G be a group. A **subgroup** H of G is a subset H of G such that (s.t.):
1) the neutral element of G belongs to H,
2) $\forall a, b \in H$ it holds that $ab \in H$,
3) $\forall a \in H$ it holds that $a^{-1} \in H$.

Remark.
- A subgroup H is called a proper subgroup of G if the set H is distinct from G, i.e. $H \neq G$.
- Any group has a trivial subgroup that is composed of the set $\{e\}$ containing only the identity element.

We now proof two useful properties of subgroups:

(2.1) Proposition.
If G is a group, $H \subset G$ is a subgroup of G if and only if
1) H is not empty,
2) $\forall a, b \in H$ it holds that $ab^{-1} \in H$.

Proof.
H subgroup $\Leftrightarrow$ (1) and (2)?

$\Rightarrow$:
H subgroup $\Rightarrow$
$e \in H \Rightarrow H$ not empty (1).
If $b \in H, b^{-1} \in H$ (because every element is invertible in H).
If $a \in H, b^{-1} \in H, ab^{-1} \in H$ (because H is closed) (2).

$\Leftarrow$: We have to proof that H is closed and contains the neutral and inverse elements.
Because of (1) H is not empty, $\exists a \in H$.
$a \in H \Rightarrow aa^{-1} = e \in H$ because of (2) (therefore the neutral element $\in H$).
If $a, e \in H, ea^{-1} \in H$, then $a^{-1} \in H$ (therefore the inverse elements are $\in H$).
If $b^{-1} \in H, a \in H, a\left(b^{-1}\right)^{-1} = ab \in H$, then $ab \in H$ (closure of H). □

(2.2) Proposition.
H is a subgroup of $G \Rightarrow H$ "inherits" a group structure.

(2.3) Proposition.
Let G be a group, and H_1 and H_2 be two subgroups of G. Then $H_1 \cap H_2$ is a subgroup of G.

Proof.
(We use the alternative definition of subgroups that we have just demonstrated).
H_1 subgroup $\Rightarrow e \in H_1$.
H_2 subgroup $\Rightarrow e \in H_2$.
Therefore $e \in H_1 \cap H_2$ is not empty, i.e. condition (1) is fulfilled for $H_1 \cap H_2$.
If $a, b \in H_1 \cap H_2, ab^{-1} \in H_1 \cap H_2$?
$a, b \in H_1 \Rightarrow ab^{-1} \in H_1$ using condition (2) for H_1.
$a, b \in H_2 \Rightarrow ab^{-1} \in H_2$ using condition (2) for H_2.
Therefore $ab^{-1} \in H_1 \cap H_2$, i.e. condition (2) is fulfilled for $H_1 \cap H_2$. □

This statement can be generalized to whole families of subgroups.

(2.4) Proposition.
Let $\{H_i\}_{i \in I}$ be a subgroup family of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof.
Left to the reader.

Remark.
H_1 and H_2 subgroups $\not\Rightarrow H_1 \cup H_2 =$ subgroup.

We now turn our attention to the notion of subgroup generators.

(2.2) Definition.
Let G be a group. Let A be a subset of G.
Then the subgroup of G generated by A is (equivalently)
1) the smallest subgroup of G containing A

2) the intersection of all subgroups of G containing A
3) $\left\{\alpha_1^{\epsilon_1}\alpha_2^{\epsilon_2}\ldots\alpha_n^{\epsilon_n}\right\}_{n\in\mathbb{N}}$, $\alpha_i \in A$, $\epsilon_i = \pm 1$.

Terminology.
Let G be a group and A a subset of G. We will note $G(A)$ the subgroup of G generated by A, which is therefore the smallest subgroup of G containing A or also $\left\{\alpha_1^{\epsilon_1}\alpha_2^{\epsilon_2}\ldots\alpha_n^{\epsilon_n}\right\}_{n\in\mathbb{N}}$, $\alpha_i \in A$, $\epsilon_i = \pm 1$.

(2.5) Proposition.
The group G is finite if and only if there exists a finite subset A such that $G = G(A)$.

(2.3) Definition.
If the group G is finite and admits a generating system with only one element, it is said to be **cyclic**[5].

(2.6) Proposition.
A group $(G, \cdot)$ is a cyclic group generated by g if the only subgroup that contains g is the group $(G, \cdot)$ itself.

As groups are based on sets we can form cartesian or direct products.
Let G_1 and G_2 be the carriers of two groups (G_1, μ_1) and (G_2, μ_2).
We define the direct product $G_1 \times G_2$ as the assembly of all ordered pairs $\{(g_1, g_2)\}$ with $g_1 \in G_1$ and $g_2 \in G_2$. The direct product then forms a group. Formally:

(2.7) Proposition.
Let (G_1, μ_1), (G_2, μ_2) be two groups. Then $G_1 \times G_2$, the cartesian product, defined as

$$\begin{aligned} G &= G_1 \times G_2 \\ &= \{(g_1, g_2) \text{ such that } g_1 \in G_1; g_2 \in G_2\} \end{aligned}$$

forms a group under the binary relation

$$\mu\left((g_1, g_2), (g_1', g_2')\right) = \left(\mu_1(g_1, g_1'), \mu_2(g_2, g_2')\right).$$

The associativity of μ is guaranteed by the associativity of μ_1 and μ_2.
The identity element is given by $(e(G_1), e(G_2))$, with $e(G_1)$ and $e(G_2)$ the identity elements of G_1 and G_2, respectively.
The inverse is given by (g_1^{-1}, g_2^{-1}), with g_1^{-1} and g_2^{-1} the inverse elements of g_1 and g_2 in G_1 and G_2, respectively.

We thus can speak of the **direct group product**.

(2.8) Proposition.
The direct group product definition is coherent.

---

[5] Be careful: It is not because the group is cyclic that it is finite.
$(\mathbb{Z}, +)$ is e.g. a cyclic group that is generated by 1, but is infinite. This terminology can thus be intuitively misleading. For Bourbaki, a group generated by one element is said "monogene", and a cyclic group is a finite monogene group. Those definitions must therefore be considered with care because they are not universal.

Proof.

$$\begin{aligned}
&\mu\left((g_1,g_2),\mu\left((g_1',g_2'),(g_1'',g_2'')\right)\right)\\
&\quad=\mu\left((g_1,g_2),\left(\mu_1(g_1',g_1''),\mu_2(g_2',g_2'')\right)\right)\\
&\quad=\left(\mu_1\left(g_1,\mu_1(g_1',g_1'')\right),\mu_2\left(g_2,\mu_2(g_2',g_2'')\right)\right)\\
&\quad=\left(\mu_1\left(\mu_1(g_1,g_1'),g_1''\right),\mu_2\left(\mu_2(g_2,g_2'),g_2''\right)\right)\\
&\quad=\mu\left(\left(\mu_1(g_1,g_1'),\mu_2(g_2,g_2')\right),(g_1'',g_2'')\right)\\
&\quad=\mu\left(\mu\left((g_1,g_2),(g_1',g_2')\right),(g_1'',g_2'')\right)
\end{aligned}$$

□

3. GROUP HOMOMORPHISM, IMAGE, KERNEL

We now want to introduce functions (or applications) that map the elements of one group (objects) onto another (images). We are particularly interested in such functions that preserve the group structures. These functions are called homomorphisms. When dealing with homomorphisms we have the free choice of first combining the objects and then producing the image or equivalently of first producing the images from the objects and then combining those images.

(3.1) Definition.
Let (G_1,μ_1) and (G_2,μ_2) be two groups and $f: G_1 \to G_2$ an application.
f is called a group homomorphism if

$$\forall a,b \in G_1,\ f\left(\mu_1(a,b)\right)=\mu_2\left(f(a),f(b)\right)$$

$\Leftrightarrow$ the diagram:

$$\begin{array}{ccc}
G_1\times G_1 & \xrightarrow{\mu_1} & G_1\\
\downarrow{\scriptstyle f\times f} & \bigcirc & \downarrow{\scriptstyle f}\\
G_2\times G_2 & \xrightarrow{\mu_2} & G_2
\end{array}$$

is commutative, i.e. the two paths are equivalent (see Fig. 1). One sometimes notes this property by $\bigcirc$.

We usually say that f is compatible with both laws μ_1 and μ_2.

As they preserve the group structures, homomorphisms match the identity elements as well as the inverse elements onto each other. Formally:

(3.1) Proposition.
Let $f: G_1 \to G_2$ be a group homomorphism. Then
1) $f(e_1)=e_2$
2) $f(a^{-1})=(f(a))^{-1}$

Proof.
Statement (1)
We consider the two "paths" of the previous diagram.

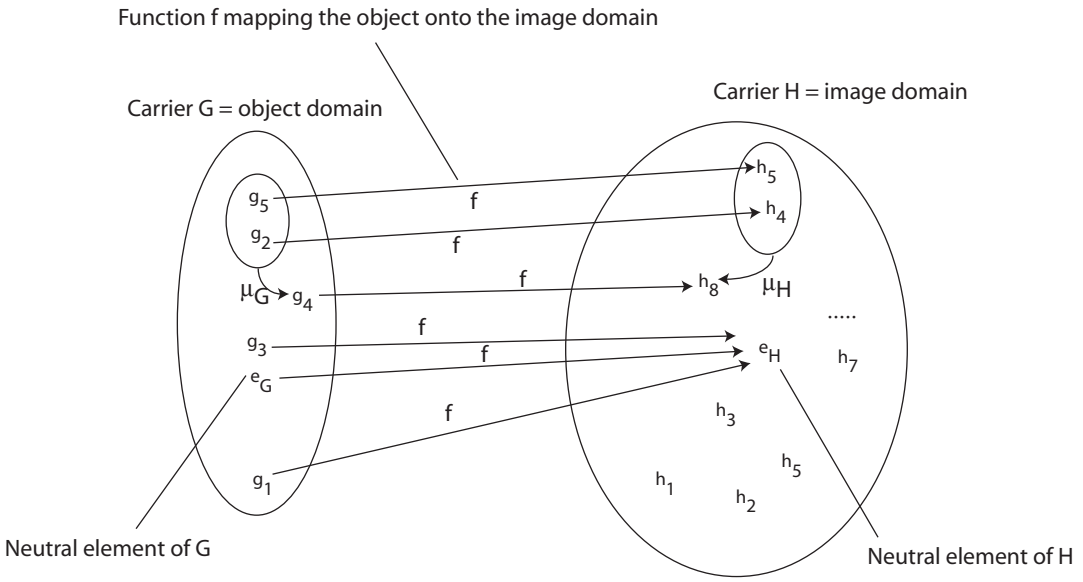


Figure 1. Schematics of a group homomorphism $f : G \to H$. To be a homomorphism the function f has to preserve the group structures. For the given example this implies among other things that if $\mu_G(g_5, g_2) = g_4$ then $\mu_H(h_5 = f(g_5), h_4 = f(g_2)) = f(g_4) = h_8$. Any object possesses a unique image. A given image can, however, be associated with various objects.

"First path": Producing the images under the function f and combining them via the relation μ_2.

$$\begin{array}{ccc} (e_1, e_1) & \longrightarrow & \\ \downarrow & & \downarrow \\ (f(e_1), f(e_1)) & \longrightarrow & f(e_1)f(e_1) \end{array}$$

"Second path": Combining the elements via the relation μ_1 and then produce the image via the function f.

$$\begin{array}{ccc} (e_1, e_1) & \longrightarrow & e_1 \\ \downarrow & & \downarrow \\ & \longrightarrow & f(e_1) \end{array}$$

f is a homomorphism. Therefore, the two paths give identical results $\Rightarrow f(e_1)f(e_1) = f(e_1e_1) = f(e_1)$
G_2 group $\Rightarrow f(e_1) = e_2$ (we multiply by $f(e_1)^{-1}$) (q.e.d).

Statement (2)
Identically, we can write the two "paths" of the diagram as follows:
"First path"

$$\begin{array}{ccc} (a, a^{-1}) & \longrightarrow & \\ \downarrow & & \downarrow \\ \left(f(a), f(a^{-1})\right) & \longrightarrow & f(a)f(a^{-1}) \end{array}$$

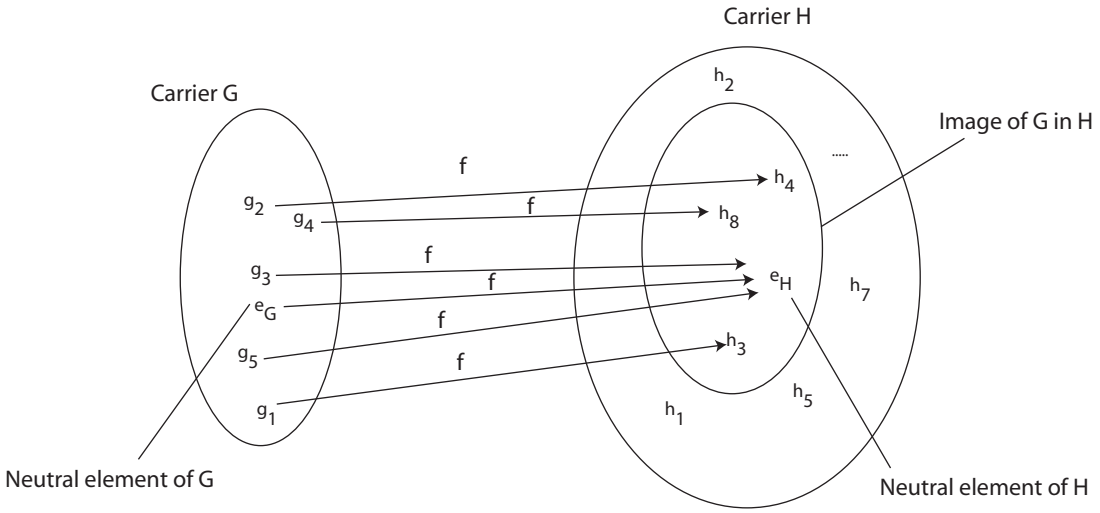


Figure 2. The image of a group homomorphism $f : G \to H$ consists of all elements in the image domain H that emanate from an element in the object domain G. The image forms a subgroup of H.

"Second path"

$$\begin{array}{ccc} (a, a^{-1}) & \longrightarrow & e_1 \\ \downarrow & & \downarrow \\ & \longrightarrow & e_2 \end{array}$$

so $e_2 = f(a)\,f(a^{-1})$, which shows that $(f(a))^{-1} = f(a^{-1})$. □

As homomorphisms preserve the group structure it is not surprising that the image they produce of the entire object group (G_1, μ_1) is in itself a group $(\mathrm{Im}(f), \mu_2)$ contained in the carrier G_2 (see Fig. 2). Formally:

(3.2) Proposition.
Let $f : G_1 \to G_2$ be a group homomorphism.
Then

$$\begin{aligned} \mathrm{Im}(f) &= \{g_2 \in G_2 \text{ such that } \exists g_1 \in G_1 \text{ such that } f(g_1) = g_2\} \\ &= \text{ image of } f \end{aligned}$$

is a subgroup of G_2.

Proof.
We note $\mathrm{Im}(f) = f(G_1)$.
$f(G_1)$ is not empty as it contains $f(e_1) = e_2$.
Let $a', b' \in f(G_1)$; do we have $a'b'^{-1} \in f(G_1)$?
We know that $a' = f(a)$ and $b' = f(b)$, $a, b \in G_1$. Therefore

$$\begin{aligned} a'b'^{-1} &= f(a)\,(f(b))^{-1} \\ &= f(a)\,f(b^{-1}) \quad \text{because } f \text{ homomorphism} \\ &= f(ab^{-1}) \qquad \text{idem} \end{aligned}$$

which shows $a'b'^{-1} \in f(G_1)$. □

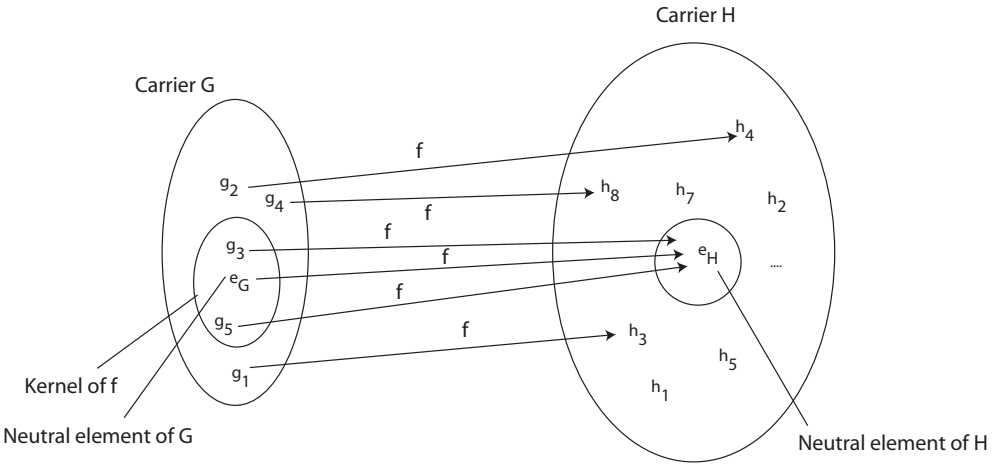


Figure 3. The kernel of a group homomorphism $f : G \to H$ consists of all elements in the object domain G that are matched on the neutral element in the image domain H. The kernel forms a subgroup of G.

(3.3) Proposition.
More generally, if $f : G_1 \to G_2$ is a group homomorphism and if H_1 is a subgroup of G_1, then $f(H_1)$ is a subgroup of G_2.

Proof.
Left to the reader.

Apart from the image, the kernel is an important characteristic of a homomorphism f. The kernel is comprised of all the elements in G_1 that are mapped by f onto the neutral element of G_2 (see Fig. 3). We thus may say that the elements of the kernel are neutralized, i.e. they are rendered inactive within G_2. Any multiplication of an object with an element of the kernel in G_1 will not change the image of that object in G_2. Formally:

(3.2) Definition.
Let $f : G_1 \to G_2$ be a group homomorphism. Then

$$\begin{aligned} \ker(\mathrm{f}) &= \{g_1 \in G_1 \text{ such that } f(g_1) = e_2\} \\ &= \text{ kernel of } f \end{aligned}$$

(3.4) Proposition.
$\ker(f)$ is a subgroup of G_1.

Proof.
$\ker(f)$ is not empty as $e_1 \in \ker(f)$.
If $a, b \in \ker(f)$, do we have $ab^{-1} \in \ker(f)$?

$$\begin{aligned} f(ab^{-1}) &= f(a)f(b^{-1}) \quad \text{as } f \text{ is a homomorphism} \\ &= f(a)\,(f(b))^{-1} \quad \text{idem} \\ &= e_2\,(e_2)^{-1} \\ &= e_2. \end{aligned}$$

Therefore, $\ker(f)$ is a subgroup of G_1. □

An extreme case of a group homomorphism is a function $f : G_1 \to G_2$ that maps all elements of G_1 onto the neural element of G_2. In that case the kernel of f is identical to G_1 and all elements of G_1 become neutralized in G_2. Such a homomorphism, therefore, leads to a complete "information loss of the object" in the image domain.

In general homomorphisms connect distinct carriers. Particular properties arise when the function f maps the carrier of the group onto itself. We now proof a couple of useful relations between such homomorphisms and the commutation property.

(3.5) Proposition.
The application $f : G \to G; a \mapsto a^2$ is a group homomorphism $\Leftrightarrow$ G is commutative.

Proof.
$\Rightarrow$: because f is an homomorphism, we can write the two paths of the following diagram:
"First path"

$$\begin{array}{ccc} (a,b) & \longrightarrow & \\ \downarrow & & \downarrow \\ \left(a^2,b^2\right) & \longrightarrow & aabb \end{array}$$

"Second path"

$$\begin{array}{ccc} (a,b) & \longrightarrow & ab \\ \downarrow & & \downarrow \\ & \longrightarrow & abab \end{array}$$

Because the diagram is commutative we have $abab = aabb \Leftrightarrow bab = abb \Leftrightarrow ba = ab$ so G is commutative.

$\Leftarrow$: If G is commutative, then $abab = aabb$ which makes the previous diagram commutative, and proves that f is a group homomorphism. □

Remark.
In general, if the group G is not commutative, the application

$$\begin{aligned} f_m : G &\longrightarrow G \\ a &\longmapsto a^m \end{aligned}$$

for a given m, is **not** a group homomorphism (for it to be true, one would need, as in the previous case, that $abab \ldots abab = aa \ldots aabb \ldots bb$).

For the following discussion we have to introduce the subgroups of $(\mathbb{Z}, +)$. We will demonstrate that these subgroups are all composed by the multiples of a unique generator $a \in \mathbb{Z}$.

(3.6) Proposition.
Let G be a subgroup of $\mathbb{Z}$. Then there exists a unique number a $(\exists! a \in \mathbb{N})$ such that $G = a\mathbb{Z} = \{\text{multiples of } a\}$.
(in other words, every subgroup of $\mathbb{Z}$ is of the form $a\mathbb{Z}$, $a \in \mathbb{N}$, and a is unique)

Proof.
If G = trivial subgroup = "null" subgroup = $\{\ 0\ \} = 0 \cdot \mathbb{Z}$, we have the result.
If not, then $\exists b \in G, b \neq 0$. Consequently, there exists $c > 0 \in G$ as if $b < 0$ then $-b \in G$ and $-b > 0$.
Let $a = \min\{b \in \mathbb{N}_* \cap G\}$. Because $a \in G, na \in G, \forall n \in \mathbb{Z}$.
If $n > 0, na = a + \ldots + a \in G$.
If $n = 0, 0 \cdot a = 0 \in G$.
If $n < 0, -na = -(na) \in G$.
Let $b \in G$; we (euclidean) divide b by a to obtain $b = qa + r$ where $r \in \{0, 1, \ldots, a-1\}$, and $r = b - qa \in G$.
Because a is the minimum, necessarily $r = 0$. We therefore have $G = a\mathbb{Z}$. □

This allows us to define in an elegant way the order of an element of a group.

(3.3) Definition.
Let G be a group, and $a \in G$. We can define the group homomorphism

$$f_a : \mathbb{Z} \longrightarrow G$$
$$n \longmapsto a^n$$

If the kernel of f_a is not empty then the unique element ω of $\mathbb{N}$ that generates $\ker(f_a) = \omega\mathbb{Z}$ is called the **order** of a in G.

$$\ker(f_a) = \left\{n \in \mathbb{Z} \text{ s.t. } a^n = e\right\}$$

The kernel of f_a is never empty if the set G is finite.

We now address the important subject of comparing group structures. Groups as we have defined them are a priori distinct as soon as they are based on different carriers, i.e. different sets of elements. Starting from a given carrier, additional groups can thus be created by a simple relabeling of the elements of the carrier while preserving the relations that exist among them. In that case we definitely would consider that the structure of all these groups is identical, i.e. that all these groups have the same algebraic form, i.e. that they are isomorphic. We extend the concept by considering two groups as **isomorphic** whenever there is a one-to-one correspondence (bijection) between the elements of the group that respects the group structure.

We will now cast this statement into a mathematical form. To this end we recall a few essential definitions characterizing functions.

A function is called **injective** if the images preserve the distinctness of the objects. Thus two distinct objects have to be mapped onto two distinct images.
Formally:
The function $f : G_1 \to G_2$ is injective if for all $a \neq b \in G_1$ it holds that $f(a) \neq f(b)$ in G_2.

It can be shown that in the case of an injective homomorphism the kernel of f has to be trivial.

(3.7) Proposition.
If $f : G_1 \to G_2$ is a group homomorphism then f is injective $\Leftrightarrow \ker(f) = \{e_1\}$.

Proof.
$\Rightarrow$: f homomorphism $\Rightarrow f(e_1) = e_2$.
f injective $\Rightarrow \forall x \neq e_1, f(x) \neq e_2$.
Consequently, $\ker(f) = f^{-1}(\{e_2\}) = \{e_1\}$.

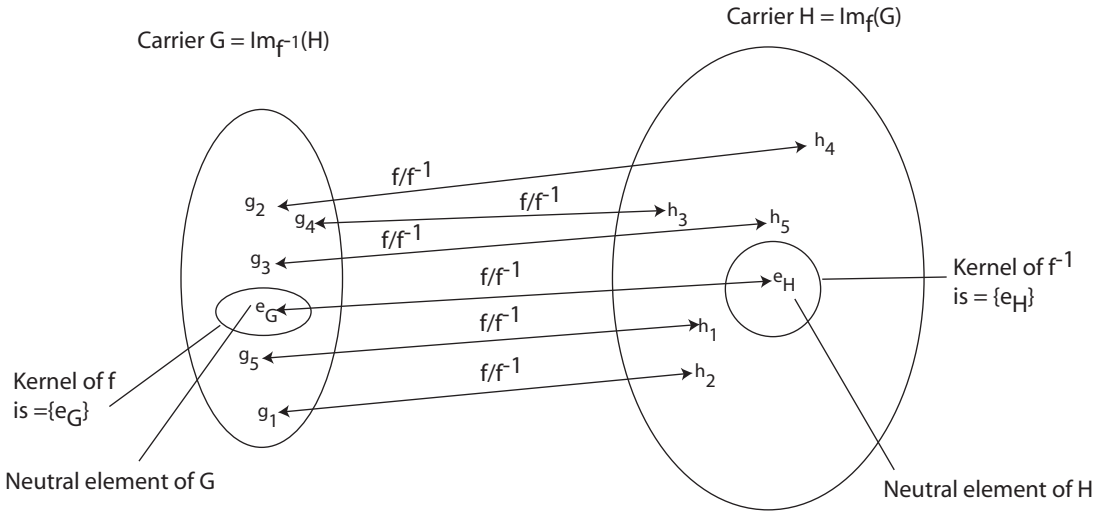


Figure 4. Schematics of a group isomorphism. There is a one-to-one correspondence of the elements that preserves the group structure, i.e. both f and f^{-1} are group homomorphisms. Both kernels have to be trivial, i.e. they contain only the respective neutral element.

$\Leftarrow : f(a) = f(b) \stackrel{?}{\Rightarrow} a = b.$
$f(a) = f(b) \Rightarrow f(a)f(b)^{-1} = e_2$. As f is a group homomorphism $f(a)f(b)^{-1} = f(ab^{-1})$. Therefore,
$f(a) = f(b) \Rightarrow f(ab^{-1}) = f(b)f(b)^{-1} = e_2$.
But ker(f) = $\{e_1\}$, so $ab^{-1} = e_1$, i.e. $a = b$. □

A function is called **surjective** if every element of the image domain is the actual image of an object in the object domain.
Formally:
The function $f : G_1 \to G_2$ is surjective if for any $b \in G_2$ there exists $a \in G_1$ such that $f(a) = b$.

A function that is both injective and surjective is called **bijective**. A bijective function creates a one-to-one relation among the objects and their images.
An injective function $f : G_1 \to G_2$ can always be rendered bijective by limiting the image domain to the image of G_1 under f, i.e. by defining
$f_{\text{reduced}} : G_1 \to \text{Im}_f(G_1), \quad f_{\text{reduced}}(a) = f(a), \forall a \in G_1.$
With this background we can define the isomorphism of groups.

(3.4) Definition.
Two groups G_1 and G_2 are isomorphic if $\exists f : G_1 \to G_2$ and $\exists g : G_2 \to G_1$ two reciprocal homomorphisms.

Thus two groups are isomorphic if there is a two-way homomorphism among them. Actually the two functions f and g are reciprocal bijections, but they are in addition group homomorphisms thus preserving in the two directions the group structure.

This definition can be cast in a slightly different form by exploiting the following proposition (see Fig. 4).

(3.8) Proposition.
If $\exists f : G_1 \to G_2$ a bijective homomorphism mapping G_1 onto G_2, then G_1 and G_2 are isomorphic.

Proof.
As $f : G_1 \to G_2$ is bijective it has an inverse f^{-1}.
Let us define $g : G_2 \to G_1$ via $g = f^{-1}$.
We now have to demonstrate that g is a group homomorphism, i.e. that:
$g(\mu_2(a,b)) = \mu_1(g(a), g(b))$.
If we set $a = f(a')$ and $b = f(b')$ then the previous question becomes:
$g(\mu_2(f(a'), f(b'))) \stackrel{?}{=} \mu_1(g(f(a')), g(f(b')))$ i.e. $g(\mu_2(f(a'), f(b'))) \stackrel{?}{=} \mu_1(a', b')$.
Let us apply f to each side of this equation. This leaves us with:
$f(g(\mu_2(f(a'), f(b')))) \stackrel{?}{=} f(\mu_1(a', b'))$ i.e. $\mu_2(f(a'), f(b')) \stackrel{?}{=} f(\mu_1(a', b'))$.
The answer to this question is yes as f is a group homomorphism.
Therefore, g is a group homomorphism. □

4. GROUP AUTOMORPHISM, INNER AUTOMORPHISM

In the preceding section we have compared groups defined on different carriers. This lead us to the central concept of group isomorphisms. Isomorphisms are extremely useful as they allow to transpose group theoretical results directly from one group to its isomorphic partners. We will now turn our attention to mappings of a set onto itself. We are particularly interested in such mappings that preserve the algebraic structure of the group. These mappings are intimately related to the concept of symmetry, which in abstract terms is the ensemble of structure preserving operations of an object.

Let us start by introducing permutations, i.e. operations that rearrange the elements of a set in a unique one-to-one fashion. Mathematically this action of rearrangement corresponds to a bijection. Permutations can be executed one after the other and the result is another permutation. This provides us with an inner *law of composition*. It is easy to show that the permutations form a group under this law.

(4.1) Definition.
Let E be a set, then the permutation group of E corresponds to the set of bijections $\sigma : E \to E$.
The group law is defined by composing ($\circ$) the bijections in the following way:

$$\sigma_i \sigma_j : a \longmapsto \sigma_i \left(\sigma_j(a)\right)$$
$$(\sigma_i \sigma_j = \sigma_i \circ \sigma_j)$$

Terminology.
For a finite set of cardinality n the permutation group is denoted by $S_n(E)$ or S_n if the nature of the carrier is of no importance.
S_n is equally termed the symmetric group of E abbreviated as $Sym(E)$.

Example: Let us take a set of three elements (a, b, c). The $3! = 6$ internal bijections forming S_3 are uniquely defined by giving the corresponding one-to-one correspondences $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$.

In the usual two-row notation (first row = starting configuration, second row gives target configuration) these bijections read:

$$\sigma_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$
$$\sigma_4 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \qquad \sigma_5 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \qquad \sigma_6 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

We e.g. verify that:
σ_1 is the neutral element of S_3.
$\sigma_2 \circ \sigma_3 = \sigma_5$ etc.

Inner bijections do not necessarily preserve a group structure. To guarantee this preservation they have to be isomorphisms. Isomorphisms of a group onto itself are called automorphisms (Aut).

(4.2) Definition.
Let G be a group. Then Aut(G) is the set of isomorphisms mapping G onto itself.

$$\mathrm{Aut}(G) = \{f : G \to G \text{ such that } f = \text{bijection} + \text{homomorphism}\}$$

Then Aut(G) is a subgroup of σ_G, the set of permutations of G.

Indeed, Aut(G) $\ni \mathrm{Id}_G$ [6] so Aut(G) $\neq \emptyset$. Moreover, if $f, g \in \mathrm{Aut}(G)$, $f, g^{-1} \in \mathrm{Aut}(G)$, the combination of two bijections is a bijection, and the combination of two homomorphisms is a homomorphism (proof left to the reader), so $fg^{-1} \in \mathrm{Aut}(G)$. Aut($G$) is, therefore, a subgroup of σ_G.

Remark.
A homomorphism of a group onto itself is called an endomorphism.

A particular type of automorphisms are related to conjugation. A conjugation is an operation of the type $g \to aga^{-1}$. The result of a conjugation is non-trivial, i.e. it gives a result different from g, if g modifies the system such that the inverse a^{-1} does not annihilate the action of a. This can only be the case if a and g do not commute.

A telling example is to be found on wikipedia: let a be the action "put shoe on" and g correspond to "take sock off". Then the conjugate of g under a is: aga^{-1} = "take shoe off (= inverse of put shoe on), take sock off, put shoe on". This is definitely not equal to the action "take sock off" as putting shoes on and taking socks off do not commute.
A more physical example are rotations.
Let g equal "rotation by 180 degrees around $\hat{y}$".
Let a equal "rotation by 90 degrees around $\hat{x}$".
In that case aga^{-1} gives a "180 degree rotation around $\hat{z}$", which is distinct from g. This is not surprising as rotations about distinct axes do not commute.

(4.1) Proposition.
Let G be a group and $a \in G$. Then Int_a defined by

$$\begin{aligned} \mathrm{Int}_a : G &\longrightarrow G \\ g &\longmapsto aga^{-1} \end{aligned}$$

is an automorphism of G.

Proof.
Int_a is indeed a homomorphism:

$$\begin{array}{ccc} (g,h) & \longrightarrow & gh \\ \downarrow & & \downarrow \\ & & aghha^{-1} \\ & & \| \\ (aga^{-1}, aha^{-1}) & \longrightarrow & aga^{-1}aha^{-1} \end{array}$$

[6] Id_G is the trivial homomorphism that maps every $g \in G$ onto itself. It is obviously a bijection.

(because the previous diagram is commutative), and moreover:

$$g \xrightarrow[\text{Int}_a]{} aga^{-1} \xrightarrow[\text{Int}_{a^{-1}}]{} a^{-1}aga^{-1}a = g$$
$$g \xrightarrow[\text{Int}_{a^{-1}}]{} a^{-1}ga \xrightarrow[\text{Int}_a]{} aa^{-1}gaa^{-1} = g$$

So $\text{Int}_{a^{-1}} \circ \text{Int}_a = \text{Int}_a \circ \text{Int}_{a^{-1}} = \text{Id}_G$, which means that $(\text{Int}_a)^{-1} = \text{Int}_{a^{-1}}$.
Int_a is injective: $ag_1a^{-1} = ag_2a^{-1} \Rightarrow ag_1 = ag_2 \Rightarrow g_1 = g_2$.
Int_a is surjective: $\forall g \in G, g = aa^{-1}gaa^{-1} = \text{Int}_a(a^{-1}ga)$.
So Int_a is a bijection. □

(4.2) Proposition.
$\{\text{Int}_a\}_{a\in G}$, the set of bijective homomorphisms when a takes its values in G, is a subgroup of $\text{Aut}(G)$.

Proof.
$\text{Int}_e = \text{Id}_G \in \{\text{Int}_a\}_{a\in G} \neq \emptyset$.
Let Int_a and $\text{Int}_b \in \{\text{Int}_a\}_{a\in G}$; then $(\text{Int}_b)^{-1} = \text{Int}_{b^{-1}}$.
Consequently, $\text{Int}_a \circ (\text{Int}_b)^{-1} = \text{Int}_a \circ \text{Int}_{b^{-1}} = \text{Int}_{ab^{-1}} \in \{\text{Int}_a\}_{a\in G}$.
So $\text{Int}(G) = \text{Aut}_{\text{Int}}(G) \subset \text{Aut}(G) \subset \sigma_G$. □

In other words, $\{\text{Int}_a\}_{a\in G}$ is the set of inner automorphisms of G, which we also denote by $\text{Aut}_{\text{Int}}(G)$, and is a subgroup of the automorphisms of G, which is in itself a subgroup of the permutations of G.

Remark.
G commutative $\Rightarrow$ every inner automorphism is reduced to the identity. ($g \mapsto aga^{-1} = aa^{-1}g = g$).

5. EQUIVALENCE RELATIONS

In this section we turn our attention to the notion of equivalence. This will help us to structure a group in terms of subsets or classes. In the first instance we make abstraction from the group structure and treat the partitioning of a set into subunits.

We start with the definition of the **power set**.

(5.1) Definition.
Given a set E the power set $\mathcal{P}(E)$ comprises all the subsets of E.

Power sets are of essential importance in set theory.

Example : $E = \{a, b, c\}$, then $\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Terminology.
The cardinality of a set is loosely speaking the number of its elements. We denote it by $\#E$.

If the cardinality of a set is finite then the cardinality of the power set can be determined as $\#\mathcal{P}(E) = 2^{\#E}$.

In the case of infinite sets the cardinality of the power set is always greater than the cardinality of the set itself. We can e.g. establish a one-to-one correspondence between the power set of the natural numbers (that are countably infinite) with the real numbers (that are uncountably infinite).

A **partition** of a set is a subset of the power set with the property that every element of the set is uniquely attributed to a subset of the partition.

Example of partition of E: $\Pi = \{\{a\}, \{b, c\}\}$
Example of non-partition of E: $\{\{a\}, \{a, c\}, \{c\}\}$. Indeed, a and c belong to two different subsets, while b is not represented in any subset.

(5.2) Definition.
A partition of E is a set Π of subsets of E ($\Pi \subset \mathcal{P}(E)$ or also $\Pi \in \mathcal{P}(\mathcal{P}(E))$) such that:
1) $\forall A \in \Pi, A \neq \emptyset$
2) $\forall A, B \in \Pi, A \cap B \neq \emptyset \Rightarrow A = B$
3) $\bigcup_{A \in \Pi} A = E$

A typical example is the partitioning of the land mass of the globe into countries.
Attention: Countries do not partition the full globe as the oceans are to a large extent international territory. Adding international territory to the set of national countries would allow to reestablish a partitioning.

Remark.
E a set. Then a partitioning $\mathcal{P}(E)$ is also a set.

By definition a partition Π of E projects the elements of E into the subsets constituting the partition. In other words, every partition Π of E defines a "**canonical projection**" $\pi : E \to \Pi$ with $\pi(a) =$ the unique element $A \in \Pi$ which contains a.

As an example: all citizens of the globe are projected into sets (countries) of where they live. Nationality on the other hand is not creating a partition of the set of global citizens as there are citizens with double nationality, or no nationality at all.

The canonical projection $\pi : E \to \Pi$ is surjective. In the above example: a country without residents is no country.

As any given element of E belongs to a unique element of a partition of E it represents these elements (in the above example any citizen may represent the country where he lives).

This leads us to the following formal definition (see Fig. 5):

(5.3) Definition.
A **system of representation** for Π is an application $\rho : \Pi \to E$ such that $\pi \circ \rho = \mathrm{id}_\Pi$.
This amounts to choose $\rho(A) \in A$ for each element $A \in \Pi$.

The general assembly of the united nations is e.g. such a system of representation. It allocates to every country a delegation.

In a general partition there is no particular relation among the subsets. In the following step we will define the principle of equivalency in mathematical terms. Equivalency is an attribute that accepts only two values. Either two subsets are equivalent with respect to a certain criterium and then the corresponding equivalence relation between them is true or they are not and then it is false. This leads us to define equivalence via a binary relation.

(5.4) Definition.
Let E be a set; a **binary relation** $\mathcal{R}$ in E is an application

$$\mathcal{R} : E \times E \longrightarrow \{T = \text{true}, F = \text{false}\} = \{1, 0\}$$

A binary relation becomes an equivalence relation, when it fulfills particular properties.
First, in a coherent world everybody should be equivalent to him- or herself.
Second, equivalency is a two-way relationship. If A is equivalent to B then B has to be equivalent to A.
Third, equivalency is transmittable. If A is equivalent to B and if B is equivalent to C then A should be equivalent to C.
This leads us to the mathematical definition

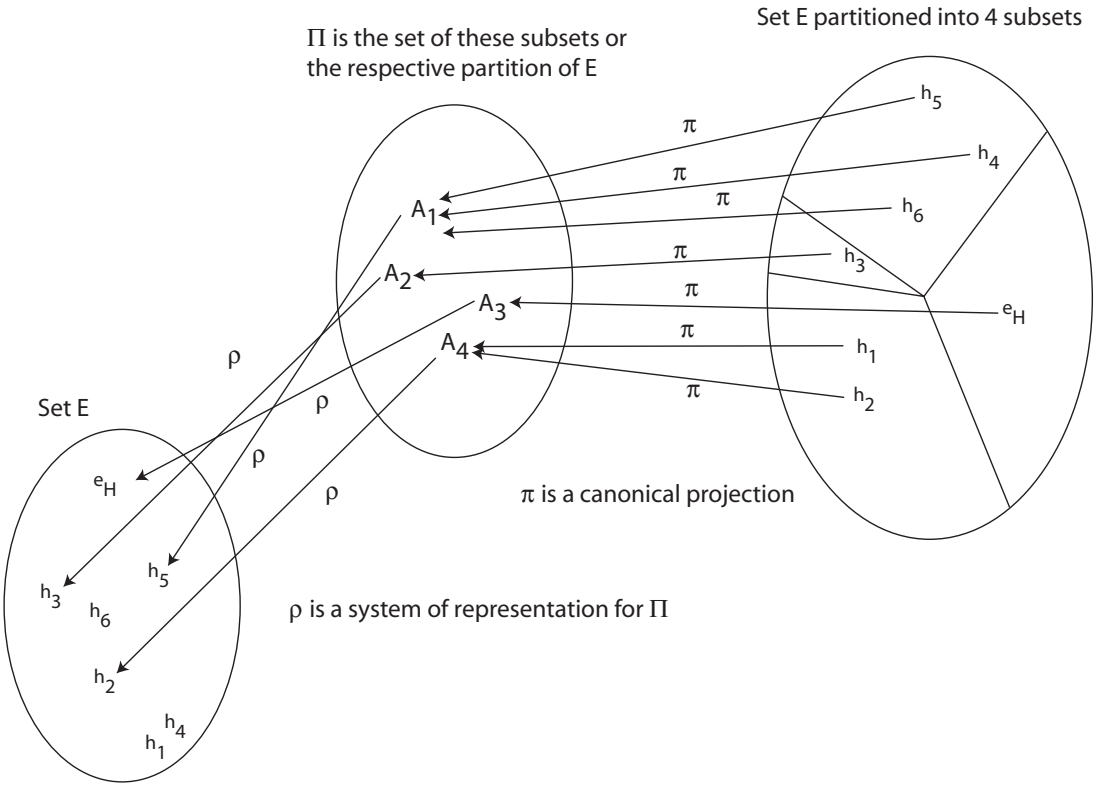


Figure 5. Schematics of a partition and a system of representatives. The partition Π has four elements. These elements are the sets $\{e_H\}, \{h_3\}, \{h_1, h_2\}, \{h_4, h_5, h_6\}$. Every element of E is uniquely mapped onto the partition via the canonical projection π. On the other hand the partition may be represented by anyone of the members of the sets that it is containing. The mapping $\rho : A_1 \to h_5, A_2 \to h_3, A_3 \to e_H, A_4 \to h_2$ is such a system of representatives.

(5.5) Definition.
A binary relation $\mathcal{R}$ is an **equivalence relation** if:
1) (reflexivity) $\forall a;\ \mathcal{R}(a,a) = T$,
2) (symmetry) $\forall a, b;\ \mathcal{R}(a,b) = T \Rightarrow \mathcal{R}(b,a) = T$,
3) (transitivity) $\forall a, b, c;\ \mathcal{R}(a,b) = T$ and $\mathcal{R}(b,c) = T \Rightarrow \mathcal{R}(a,c) = T$.

Remark.
A relation that is reflective, transitive and anti-symmetric, i.e. for which
$\forall a, b;\ (\mathcal{R}(a,b) = T$ and $\mathcal{R}(b,a) = T) \Rightarrow a = b$
is called a "partial order" (example: if $a > b$ and $b > a$ then $a = b$).

Terminology.
The above notation can become cumbersome. Often $\mathcal{R}(a,b) = T$ is simply replaced by $a \sim b$ indicating that a is equivalent to b.

Equivalence relations allow to partition a set E into **equivalence classes**.

(5.6) Definition.
Let E be a set and $\mathcal{R}$ an equivalence relation. Then if $a \in E$, the equivalence class of a modulo $\mathcal{R}$ is the set

$$\bar{a}^R = \{b \in E | \mathcal{R}(a,b) = T\}.$$

(5.1) Proposition.
The set of equivalence classes $\{\bar{a}^R | a \in E\}$ is a partition Π of E.

Proof.
Three conditions have to be satisfied:
(1) None of the equivalent classes is empty as every element a is equivalent to itself. Therefore, $\{a\} \subset \bar{a}^R$ and in consequence $\bar{a}^R \neq \emptyset$.
(2) As a is equivalent to itself any element $a \in E$ belongs to an equivalence class. Therefore, $\bigcup_{A \in \Pi} A = E$.
(3) This membership is unique. Let $c \in \bar{a}^R$ and at the same time $c \in \bar{b}^R$. Then, $\mathcal{R}(a,c) = T$ and $\mathcal{R}(b,c) = T$. As $\mathcal{R}$ is transitive and symmetric this implies that $\mathcal{R}(a,b) = T$ and, therefore, $\bar{a}^R = \bar{b}^R$. Therefore, $\forall \bar{a}^R, \bar{b}^R \in \Pi$, $\bar{a}^R \cap \bar{b}^R \neq \emptyset \Rightarrow \bar{a}^R = \bar{b}^R$. □

(5.2) Proposition.
Let G be a group and H a subgroup of G. Then H defines two equivalence relations

$$\mathcal{R}_l^H(a,b) = T \Leftrightarrow a^{-1}b \in H$$

$$\mathcal{R}_r^H(a,b) = T \Leftrightarrow ab^{-1} \in H.$$

Terminology.
We call $\mathcal{R}_l^H$ the set of **left equivalence classes** modulo H of G. This set is denoted by G/H.
$\mathcal{R}_r^H$ is the set of **right equivalence classes** modulo H of G and is denoted by $H\backslash G$.
When it comes to groups, one uses "coset" instead of equivalence class; therefore, we will from now on speak of **right cosets** and **left cosets**.

Proof.
Part I of the proposition: $\mathcal{R}_l^H$ is an equivalence relation.
1) $\mathcal{R}_l^H(a,a) = T \Leftrightarrow a^{-1}a \in H$ but $a^{-1}a = e \in H$: $\mathcal{R}_l^H$ is reflexive.
2) $\mathcal{R}_l^H(a,b) = T \Leftrightarrow a^{-1}b \in H$, but H is a subgroup so $\left(a^{-1}b\right)^{-1} = b^{-1}a \in H$, i.e. $\mathcal{R}_l^H(b,a) = T$: $\mathcal{R}_l^H$ is symmetric.
3) If $a^{-1}b \in H$ and $b^{-1}c \in H$ then H subgroup implies $a^{-1}bb^{-1}c = a^{-1}c \in H$: $\mathcal{R}_l^H$ is transitive.
The fulfillment of these three conditions characterizes $\mathcal{R}_l^H$ as an equivalence relation.

Part II of the proposition: $\mathcal{R}_r^H$ is an equivalence relation (following the same derivation, we obtain the same conclusion for $\mathcal{R}_r^H$). □

(5.3) Proposition.
Let G be a group and H a subgroup of G. Then the (unique) left coset of H in G containing a is

$${}^H\bar{a}^l = aH = \{ah \text{ with } h \in H\}$$

and identically (for the (unique) right coset H in G containing a)

$${}^H\bar{a}^r = Ha = \{ha \text{ with } h \in H\}$$

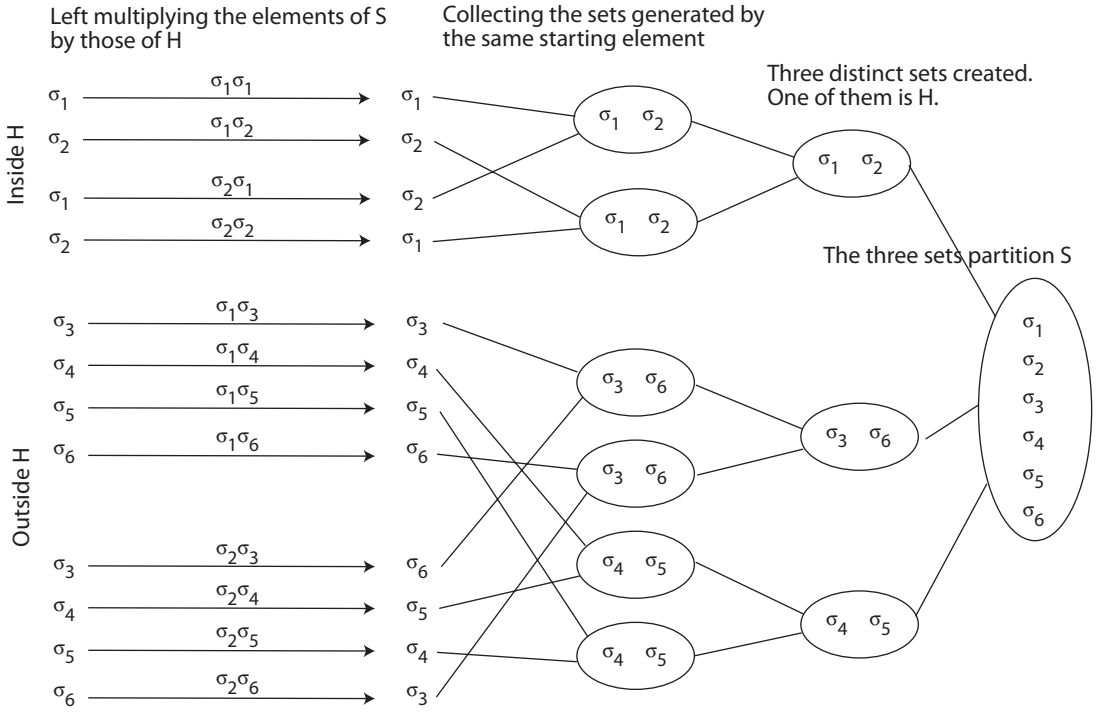


Figure 6. Schematics of the operations leading to the right cosets of the permutation group S of three elements with respect to the subset $H = \{\sigma_1, \sigma_2\}$ (see text). All elements of the group are systematically left multiplied by the two elements of H. The results corresponding to each element are grouped in 6 subsets. Out of these six, three are distinct. These three sets partition S. Only one of the sets H is a group.

Proof.

$$\mathcal{R}_l^H(a,b) = T \Leftrightarrow \exists h \in H \text{ s.t. } a^{-1}b = h$$
$$\Leftrightarrow \exists h \in H \text{ s.t. } b = ah.$$

□

Example.

Let us take as an example the group of permutations of 3 elements that we had already encountered in section 4.

We choose as the subgroup H the permutations σ_1 and σ_2. σ_1 is the neutral element and has to be in H. σ_2 permutes the elements b and c and is by definition its own inverse.

Left multiplying the elements of H by the group elements gives three left cosets.

- The first one is identical to H and thus is a subgroup of G.
- The second coset is $\{\sigma_3, \sigma_5\}$. It does not contain the neutral element and thus cannot be a subgroup of G.
- The third coset is $\{\sigma_4, \sigma_6\}$. Idem.
- All three left cosets together give the group G.

We get a different set of right cosets (See Fig. 6).

- The first one is identical to H and thus is a subgroup of G.
- The second coset is $\{\sigma_4, \sigma_5\}$. It does not contain the neutral element and thus cannot be a subgroup of G.

• The third coset is $\{\sigma_3, \sigma_6\}$. Idem.
If we had chosen a different subgroup we would have naturally obtained different cosets.

Remark.
If the group law is commutative, then $\mathcal{R}_l^H = \mathcal{R}_r^H$.

(5.4) Proposition.
Let G be a group and H a subgroup of G. Then every left coset aH can be mapped bijectively onto H. Idem for right cosets.

This implies that there is a one-to-one correspondence between the elements of a coset and those of the generating subgroup.

Proof.
We demonstrate this proposition explicitly by constructing bijective applications.
Let $\tau_a^l : H \to aH; h \mapsto ah$: this is the left translation by a.
Its reciprocal application is $\tau_{a^{-1}}^l : aH \to H; ah \mapsto h$.
Idem for the other applications τ_a^r and $\tau_{a^{-1}}^r$. □

(5.1) Corollary.
If G is a finite group and H is a subgroup of G, then $\#H|\#G$.

Proof.
G/H is a partition of G into m cosets.
Due to the existence of the aforementioned bijective applications each coset has the same cardinality n as the generating subgroup H.
Therefore, $\#G = m \cdot n$, which means $n \mid \#G$.
(this is the so called Lagrange theorem) □

Let G be a group and H a subgroup of G. Then we can partition G in cosets: G/H for instance. We may now ask the question: Is it possible to endow the set of cosets G/H with a group structure?
The *natural way* to tackle this question is by trying to transpose the group properties of G to the set of cosets. In other words, for $\bar{a} = aH \in G/H$ and for $\bar{b} = bH \in G/H$, we would like to define the product, $\bar{a} \cdot \bar{b} := (ab)H = \overline{(ab)}$.

Warning: We have to verify the coherence of such a definition, i.e. we have to make sure that the product does not depend on the particular choice of the representatives a and b used to characterize each coset. Therefore, we must check that if $aH = a'H$ and $bH = b'H$ then $abH = a'b'H$.

$aH = a'H$ and $bH = b'H$ implies:

$$aH = a'H \Leftrightarrow \exists h \in H \text{ s.t. } a' = ah$$
$$bH = b'H \Leftrightarrow \exists h' \in H \text{ s.t. } b' = bh'$$

We have to check whether the relation $\mathcal{R}_l^H(ab, a'b')$ is true, i.e. whether $(ab)^{-1}a'b' \in H$?
Using the above statements we can write $a'b' = ahbh'$.

As $(ab)^{-1} = b^{-1}a^{-1}$ we obtain $(ab)^{-1}(a'b') = b^{-1}a^{-1}ahbh' = b^{-1}hbh'$.
Thus $(ab)^{-1}a'b' \in H$ provided that $b^{-1}hb \in H$.

There is no general reason why this should be the case.

This leads us to the following definition:

(5.7) Definition.
Let G be a group and H a subgroup of G. H is a **normal subgroup** if

$$\forall a \in G, aHa^{-1} = H$$

or equivalently

$$\forall h \in H, aha^{-1} \in H.$$

In other words, H is normal (in G) $\Leftrightarrow$ H is globally invariant under the action of any inner automorphism.

Remark.
Normal subgroups H are thus invariant under the operation of conjugation in G.

With the definition of the normal subgroups we have attained our goal of endowing the set of cosets with a canonical (i.e. inherited) group structure.
Formally:

(5.1) Theorem.
Let G be a group and H a normal subgroup.
1) $\forall a \in G,\ aH = Ha$, i.e. left cosets equal right cosets.
2) $G/H = H\backslash G$, is canonically endowed with a group structure, called the quotient structure.

Proof.
1) $\forall a \in G,\ aH = Ha$?
Because H is normal in G, $\forall a \in G,\ aHa^{-1} = H$; i.e. $\forall a \in G,\ \forall h \in H,\ \exists h' \in H$ such that $aha^{-1} = h'$, or equivalently, $ah = h'a$. So $aH \subset Ha$. The reciprocal implication is proved following the same directions, so $aH = Ha$.

2) $G/H = \{aH\} = \{Ha\}$
Coherence of the definition: If $aH * bH = (ab)H$ and if $a'H * b'H = (a'b')H$, do we have $(ab)H = (a'b')H$?
We have $a^{-1}a \in H$ and $b^{-1}b' \in H$ and we ask ourselves if we will end up with $(ab)^{-1}(a'b') \in H$?
$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b'$ but $a' = ah$ and $b' = bh'$ so $b^{-1}a^{-1}a'b' = b^{-1}a^{-1}ahbh' = (b^{-1}hb)h'$ and because the subgroup H is normal in G (and this is precisely for that reason that we need it to be), we have a $b^{-1}hb \in H$, i.e. $b^{-1}hb = h'' \in H$. Consequently, $(ab)^{-1}(a'b') = h''h' \in H$ and the definition is coherent.

Is the law associative?
$(aH)((bH)(cH)) = (aH)((bc)H) = (a(bc))H = ((ab)c)H = ((aH)(bH))(cH)$, so the law is associative.
Neutral element: $eH = H =$ "neutral class" or "neutral coset" in G/H.

Inverse: $(a\,H)^{-1} = a^{-1}H$

We therefore have a group structure. □

Terminology.
The subgroup that contains only the neutral element $\{e\}$ is a trivial normal subgroup of G.
The quotient group is equally called the factor group.
G/H is pronounced as G mod(ulo) H. The quotient group of $\{e\}$ is isomorphic to the group G itself.
If a group G has only $\{e\}$ and G as normal subgroups it is called simple.

Remark.
If G is commutative, then every subgroup H is normal.

Example.
Let us consider $(\mathbb{Z}, +)$ the group of integers under addition.
For any positive number $n \in \mathbb{Z} > 0$ we get a subgroup $n\mathbb{Z}$ consisting of all the multiples of n.
As the addition is commutative these subgroups are normal.
The cosets of $n\mathbb{Z}$ are given by the set $\{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-2) + n\mathbb{Z}, (n-1) + n\mathbb{Z}\}$.
Any integer m belongs to one of the cosets of $n\mathbb{Z}$. To identify this coset we have to determine the remainder when dividing m by n.
The cosets are therefore equally called remainder classes modulo n.
The quotient group $\mathbb{Z}/n\mathbb{Z}$ forms a cyclic group of order n.
The neutral element of the quotient group is $n\mathbb{Z}$.
If $n = 2$ we get the partitioning of $\mathbb{Z}$ into odd and even numbers.

Example.
In the following example we would like to exemplify the class structure introduced by conjugation into the symmetry group of rotations. Let us start with the free rotation group $\{R_{\hat{a}}(\alpha)\}$. In this notation the unit vector $\hat{a}$ gives the rotation axis and α the rotation angle. Two rotations $R_{\hat{a}}(\alpha)$ and $R_{\hat{b}}(\beta)$ are in the same conjugacy class if there exists a rotation $R_{\hat{c}}(\gamma)$ such that

$$R_{\hat{b}}(\beta) = R_{\hat{c}}(\gamma) R_{\hat{a}}(\alpha) R_{\hat{c}}(\gamma)^{-1}.$$

It is left as an exercise to demonstrate that this identity is only fulfilled if

$$\beta = \alpha$$

and

$$\hat{b} = R_{\hat{c}}(\gamma)\hat{a}.$$

Conjugation thus simply turns the rotation axis. All rotations about the same angle α end up in the same conjugacy class $C(\alpha)$. Thus classification reduces the dimensions from 3 (the two angles defining the direction of $\hat{a}$ plus the rotation angle α) to one (rotation angle α). Attention: the conjugacy classes partition the free rotation group. However, apart from the one for $\alpha = 0$ (trivial subgroup), they are not subgroups and as such do not factorize $\{R_{\hat{a}}(\alpha)\}$.
This result can immediately be transposed to groups of finite rotations. Let us consider the rotation group D_3 of an equilateral triangle in $\mathbb{R}^3$. There are 6 symmetry elements in that group

$$\{e = R(0),\, R_{\hat{z}}(2\pi/3),\, R_{-\hat{z}}(2\pi/3),\, R_{\hat{y}}(\pi),\, R_{\sqrt{3/4}\hat{x}+0.5\hat{y}}(\pi),\, R_{-\sqrt{3/4}\hat{x}+0.5\hat{y}}(\pi)\}$$

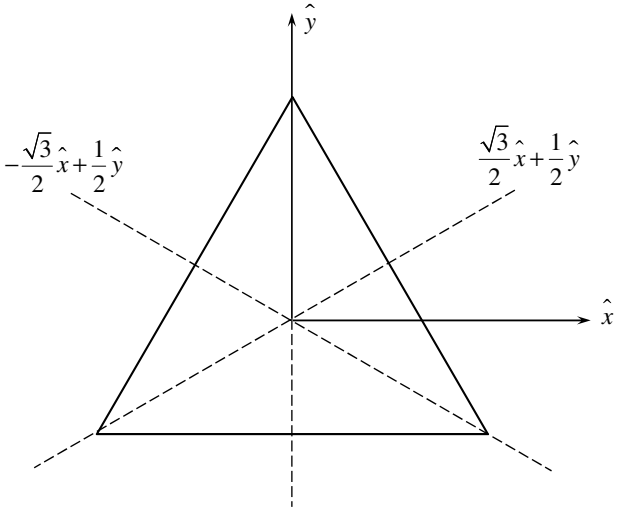


Figure 7. Symmetry elements of an equilateral triangle in $\mathbb{R}^3$.

(see figure 7). The set of rotations decomposes into three classes

$$\begin{aligned} C(0) &= \{e\}, \\ C(2\pi/3) &= R_{\hat{z}}(2\pi/3), R_{-\hat{z}}(2\pi/3), \\ C(\pi) &= R_{\hat{y}}(\pi), R_{\sqrt{3/4}\hat{x}+0.5\hat{y}}(\pi), R_{-\sqrt{3/4}\hat{x}+0.5\hat{y}}(\pi). \end{aligned}$$

In a single class we find regrouped the rotations about the same angle:
$C(0)$ is the trivial class containing the identity element (rotation by a zero angle).
$C(2\pi/3)$ features the $2\pi/3$ rotations about the $\hat{z}$ and $-\hat{z}$ directions.
$C(\pi)$ contains the π rotations about the three symmetry axes lying in the plane of the triangle.

The rotation axes in one class are all related via symmetry elements in D_3 not belonging to the respective class:
The π-rotation about $\hat{y}$ maps $\hat{z}$ onto $-\hat{z}$.
The π-rotation axes in the plane are related to each other via the $2\pi/3$-rotations about $\hat{z}$ and $-\hat{z}$.

Classification schemes of this kind are omnipresent in crystallography as can be seen in practically all chapters of this book.

Example.
We provide an additional example directly related to the symmetry groups of crystals, including factorization.

As described in great detail in the chapter by Grenier and Ballou, the space group G of a crystal consists of all the operations $\{R_\alpha|\vec{l}_n + \vec{\tau}_\alpha\}$ which leave the crystal lattice invariant. The $\{\vec{l}_n\}$ are general Bravais lattice vectors. The R_α are either simple point group operations, in that case the $\vec{\tau}_\alpha$ are zero, or compound operations in the form of glide planes or screw axes, in that case the $\vec{\tau}_\alpha$ are fractions of primitive translations. If $\vec{\tau}_\alpha = 0 \,\forall\, R_\alpha$ then we speak of symmorphic space groups.

To treat space groups it is certainly desirable to separate off the infinity of Bravais translations. We may be tempted to do so by considering the set of operations $\{R_\alpha|\vec{\tau}_\alpha\}$. Unfortunately, for a nonsymmorphic space group $\{R_\alpha|\vec{\tau}_\alpha\}$ does not necessarily form a subgroup of the space group. However,

since the translations $\{\vec{l}_n\}$ form an invariant subgroup T of the group G we may form the factor group G/T. The (right) cosets of T are given by

$$C_\alpha :=^T \overline{(R_\alpha + \vec{\tau}_\alpha)}^l = (R_\alpha + \vec{\tau}_\alpha)T = \{(R_\alpha|\vec{l}_n + \vec{\tau}_\alpha)\}.$$

As translations commute with all elements of the space group, T is a normal subgroup of G and the right cosets are thus identical to the left cosets. The cosets or classes of the factor group thus contain for every operation $(R_\alpha|\vec{\tau}_\alpha)$ the infinite ensemble of operations obtained by applying $(R_\alpha|\vec{\tau}_\alpha)$ to the original plus all the translated lattices. The factor group itself is isomorphic to the point group composed by the rotations $\{R_\alpha\}$ contained in the space group. It thus has a very reduced order. By working with the cosets we have effectively factored out the translational part of the problem.

We now formulate a few propositions that relate normal and quotient groups to homomorphisms.

(5.5) Proposition.
If $f : G \to H$ is a group homomorphism, then $\ker(f)$ is a normal subgroup of G.

Proof.
Let $a \in G,\ h \in \ker(f)$: Do we have $aha^{-1} \in \ker(f)$?

$$\begin{aligned} f(aha^{-1}) &= f(a)f(h)f(a^{-1}) \\ &= f(a)e_H f(a)^{-1} \\ &= f(a)f(a)^{-1} \\ &= e_H \end{aligned}$$

Therefore, $aha^{-1} = h' \in \ker(f)$. □

Remark.
The image $f(G)$ is a subgroup but not a normal subgroup of H. For instance, $G = O_2(\mathbb{R})$ and $H = GL_2(\mathbb{R})$.[7] Let $f : G \to H$; $A \mapsto A$, then $f(G) = G$, which is not normal in H.

(5.6) Proposition.
Let G be a group, H a normal subgroup. Then there exists a canonical projection $\pi : G \to G/H$ which is a surjective group homomorphism.

Proof.
The canonical projection is given by:
$\pi : G \to G/H$ = { cosets } = partition of G, defined by $\pi : g \mapsto g$ coset of H in $G = {}^H\overline{g}^l = {}^H\overline{g}^r = gH = Hg$.
To proof that π is a homomorphism we have to show that the π diagram is commutative.

[7] The orthogonal group $O_2(\mathbb{R})$ or $O(2,\mathbb{R})$ of degree 2 over the field $\mathbb{R}$ is the group of 2×2 orthogonal real matrices. The special linear group $SL_2(\mathbb{R})$ or $SL(2,\mathbb{R})$ of degree 2 is the set of 2×2 invertible matrices, together with the operation of ordinary matrix multiplication.

Let $g, g' \in G$:
"First path"

$$\begin{array}{ccc} (g,g') & \longrightarrow & gg' \\ \downarrow & & \downarrow \pi \\ & \longrightarrow & gg'H \end{array}$$

"Second path"

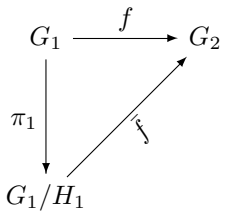
$$\begin{array}{ccc} (g,g') & \longrightarrow & \\ {\scriptstyle \pi\times\pi}\downarrow & & \downarrow \\ (gH\cdot g'H) & \longrightarrow & (gH)(g'H) \end{array}$$

and because $gHg'H = gg'H$, the diagram is commutative; π is a group homomorphism. The fact that it is surjective is obvious. □

(5.7) Proposition.
Let G_1 and G_2 be two groups, H_1 a normal subgroup of G_1, and $f : G_1 \to G_2$ a group homomorphism.

There exists a group homomorphism $\bar{f} : G_1/H_1 \to G_2$ such that $\bar{f} \circ \pi_1 = f \Leftrightarrow H_1 \subset \ker(f)$.

One usually says that the homomorphism f can be factorized. In diagram form:



Remark.
$\ker(\pi_1) = H_1$.
The content of that statement is intuitively clear. Unless H_1 is the trivial normal group of G_1 the quotient group G_1/H_1 will have a lower cardinality than G_1. Mapping G_1 onto G_1/H_1 thus implies a loss of information. In other words all information is only preserved modulo H_1 by the mapping π_1. For this loss of information not to be relevant when going from G_1 to G_2 via the detour of G_1/H_1 implies that the kernel of f (= elements of G_1 inert in G_2) comprises H_1.

We now give the formal
Proof.
$\Rightarrow$ (factorization exists)
If $f = \bar{f} \circ \pi_1$, then
$g \in H_1 \Rightarrow \pi_1(g) = \bar{e}$ (neutral element of G/H) $\Rightarrow f(g) = \bar{f} \circ \pi_1(g) = \bar{f}(\bar{e}) = e_2$ so $g \in \ker(f)$.

$\Leftarrow$ we assume $H_1 \subset \ker(f)$.
Let us define $\bar{f}(gH_1) = f(g)$.
Is this definition coherent?

Equivalently, if we take another representative for gH_1, for instance g', do we have $f(g) = f(g')$?
$f(g) = f(g') \Leftrightarrow f(g)^{-1} f(g') = e_2 \Leftrightarrow f(g^{-1}g') = e_2$. But the last relation is true because $g^{-1}g' \in H_1$.
Therefore, $\bar{f}$ is well defined.
Is $\bar{f}$ a group homomorphism?

$$\begin{aligned} \bar{f}(gH_1 \cdot g'H_1) &= \bar{f}(gg'H_1) \\ &= f(gg') \\ &= f(g)f(g') = \bar{f}(gH_1)\bar{f}(g'H_1) \end{aligned}$$

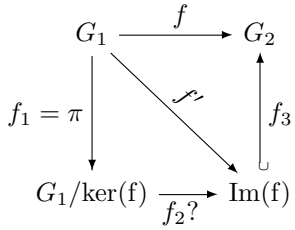
Thus the image of the product of the cosets is indeed equal to the product of the images of the cosets. □

(5.8) Proposition.
Let $f : G_1 \to G_2$ be a group homomorphism. Then there exists a canonical factorization

$$f = f_3 \circ f_2 \circ f_1$$

where
1) f_1 = surjective homomorphism
2) f_2 = isomorphism
3) f_3 = injective homomorphism

Proof.



According to the previous theorem f_2 is possible $\Leftrightarrow \ker(f') \supset \ker(f)$.
f_2 is an isomorphism because:
- f_2 is a group homomorphism.
- f_2 is by definition surjective.
- f_2 is injective $\Leftrightarrow \ker(f_2)$ = neutral element of $G_1/\ker(f) = \{ e \cdot \ker(f)\}$, which is true.

If $g\ker(f) \in G_1/\ker(f)$ and if $f_2(g\ker(f)) = e_2 \Leftrightarrow g \in \ker(f') = \ker(f)$. □

A combination of the statements proven above have gained notoriety as the first isomorphism theorem, that we will reproduce for completeness here:

(5.9) Proposition. *First isomorphism theorem*
Let G and H be groups, and let $f : G \to H$ be a group homomorphism.
Then it holds that:
- The kernel $\ker(f)$ is a normal subgroup of G
- The image $\mathrm{Im}(f)$ is a subgroup of H
- The image $\mathrm{Im}(f)$ is isomorphic to the quotient group $G/\ker(f)$.
  In particular, if f is surjective then H is isomorphic to $G/\ker(f)$.

We now establish a relation between the group of permutations S_n and n-dimensional vector spaces. This relation is of considerable importance for representation theory.

Terminology.
The set of $n \times n$ invertible matrices (with entries usually taken out of $\mathbb{R}$) forms a group under the operation of ordinary matrix multiplication.
This group is called the **general linear group** $GL_n(\mathbb{R})$. This is due to the fact that matrices describe general linear transformations. In other words, if V is a vector space then the general linear group $GL(V)$ is identical to the group of all automorphisms $Aut(V)$, which is the set of bijective *linear* transformations $V \to V$ under the operation of functional composition.

(5.8) Definition.
The **canonical representation** $\rho : S_n(E) \to GL_n(\mathbb{R})$ is the group homomorphism defined by

$$\rho(\sigma) = \left\{ e_i \longmapsto e_{\sigma(i)} \right\}$$

where

$$e_i = i^{\text{th}} \text{ base vector of } \mathbb{R}^n = (\ldots, \underset{\substack{\uparrow \\ i}}{1}, \ldots).$$

The construction of this homomorphism is such that every element in E is identified with a direction (base vector) of the vector space $\mathbb{R}^n$. The canonical equivalent of a permutation of elements transforms through ρ to a permutation of the directions in $\mathbb{R}^n$.

We thus achieve representing the permutation group S_n in a n-dimensional vector space.

ρ is indeed a group homomorphism:

$$\begin{aligned} \rho(\sigma\sigma') &= \left\{ e_i \longmapsto e_{\sigma\sigma'(i)} \right\} \\ &\text{and} \\ \rho(\sigma)\rho(\sigma') &= \left\{ e_i \longmapsto e_{\sigma'(i)} \longmapsto e_{\sigma(\sigma'(i))} \right\} \\ &= \left\{ e_i \longmapsto e_{\sigma\sigma'(i)} \right\} \end{aligned} \quad .$$

Therefore, $\rho(\sigma\sigma') = \rho(\sigma)\rho(\sigma')$.

6. GROUP ACTION

We now return to the subject of symmetry. The starting point of any symmetry consideration is an object (e.g. a cube). To be able to speak about symmetry this object has to be characterized by a set E (e.g. points in a vector space that may correspond to the vertices or edges or faces of the cube). The symmetry group of these characteristics, which may not fully describe the symmetry of the object, corresponds to the reversible transformations of the set E onto itself (e.g. permutation of the vertices, edges, faces). The elements of E are thus given by the bijective maps of the set E. If the set E is finite we usually speak of permutations in the other cases we prefer to stay with the broader notion of transformation. Symmetries described in this way are strongly linked to the underlying set. If we e.g. color the faces of the cube then the full symmetry will be reduced without affecting the symmetry of the geometrical characteristics. On the other hand the symmetry groups related to various aspects of these geometrical characteristics like vertices, edges and faces are all identical. It is thus comprehensible that we would like to have a more comprehensive description of the symmetry, i.e. we would like to decouple the notion of symmetry as much as possible from the sets. This is particularly important, when we deal with abstract symmetries. In that case it is essential to be able to establish the link with the real word, i.e. we have to be able to

transpose the symmetry properties to various sets without touching the symmetry group itself. In other words: We would like to define the action of group elements (i.e. transformations) on sets. This is the objective of this section.

How group operations (e.g. rotations in $\mathbb{R}^3$) act upon objects (e.g. scalar functions $f(\vec{r}), \vec{r} \in \mathbb{R}^3$) depends on the specific relation between them. The group actions thus have to be defined case by case. However, all of them have to fulfill at the very least the following two criteria.

- First criterium: To make any sense the action has to comply with the group structure. If we first act upon x with $g_1 \in G$ and then with $g_2 \in G$ and if $g_2 \cdot g_1 = g_3$ then the result of their combined action has to correspond to the action of g_3 upon x.
- Second criterium: The identity operation $e \in G$ should leave any element $x \in E$ invariant.

(6.1) Definition.
An action α of a group G on an ensemble E is an application

$$\alpha : G \times E \to E$$

which verifies

$$(1)\ \forall g, g' \in G,\ \forall x \in E,\ \alpha\left(g, \alpha(g', x)\right) = \alpha\left(gg', x\right),$$
$$(2)\ \forall x \in E,\ \alpha(e, x) = x.$$

Terminology.
Using the multiplicative convention for noting α, one obtains
(1) $g(g'x) = (gg')x$
(2) $ex = x$
Written in that way the group action α resembles an external law defined on E, with "coefficients" taken in G.
The set E is called a (left) **G-set**.
Left refers to the order in which the product (gg') acts on x (first g' then g).
We can equivalently define right G-sets. As right actions can always be converted into left actions with the help of the inverse elements it is sufficient to treat one of the two cases.

Example.

- Let us define a set E that describes a "Square" via the vectors $\{\ e_1, e_2, -e_1, -e_2\ \}$, where (e_1, e_2) denote the canonical basis of $\mathbb{R}^2$.

  Let us consider the group of linear transformations G that map the Square onto itself:
  $G = \{A \in GL_2(\mathbb{R})$ s.t. $A(\text{Square}) = \text{Square}\}$.
  This is the so-called symmetry group of our object.

  If we denote $a = \text{rot}_{\pi/2} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $b = \text{sym}_{Ox} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$,

  then the elements of G are:

$$id = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\ a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\ a^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\ \ a^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\ ab = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\ a^2b = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\ a^3b = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

which means that $\#G = 8$ and that:

$$G = \left\{id, a, a^2, a^3, b, ab, a^2b, a^3b\right\}$$

To perform calculations in this set, it is sufficient to know that $ba = a^3b$.
The group acts on the square in a natural way. We just specify how each of the vectors making up the set "Square" transforms under the applications making up the symmetry group G.
Formally:

$$G \times \text{Square} \longrightarrow \text{Square}$$
$$(g, \pm e_i) \longmapsto g \cdot (\pm e_i)$$

G is the dihedral group with eight elements, D_8.[8]

- When confronted with symmetry in physics we are most often concerned with transformations in space and time. Physical objects are generally described as one or multidimensional fields in the space and time variables. It is thus of paramount importance to know how the space time transformations act upon these fields.
  Let us consider the case of quantum mechanical wave functions and coordinate transformations $\{g_a\}$ in $\mathbb{R}^3$. We know how a coordinate transformation g_a acts on the space variables $(\vec{r}_1, \ldots, \vec{r}_N)$ of the wave functions (N is the number of particles).[9] The action of changing the coordinate system on a function corresponds to keeping the functional form and back-transforming the space variables. This allows us to define operators $T(g_a)$ in the Hilbert space H of the wave functions via

$$T(g_a)\psi(\vec{r}_1, \ldots, \vec{r}_N) = \psi'(\vec{r}_1, \ldots, \vec{r}_N) = \psi(g_a^{-1}\vec{r}_1, \ldots, g_a^{-1}\vec{r}_N).$$

  $T(g_a)$ expresses the action of the group element g_a on the wave functions in Hilbert space H in functional form

$$T : G \times H \to H$$
$$(g_a, \psi) \mapsto T(g_a)\psi$$

  Instead of transforming the wave functions we may equally well transform the operators $\{A\}$ in Hilbert space. To stay coherent with the action on the wave function the action of the group on the operators has to take the form

$$A' = T(g_a)AT^{-1}(g_a).$$

(6.2) Definition.
A group action $\alpha : G \times E \to E$
is effective if $\forall g \in G, g \neq e,\ \exists x \in E$ s.t. $g \cdot x \neq x$
is transitive if $\forall x, y \in E,\ \exists g \in G$ s.t. $g \cdot x = y$
is free if $\forall x \in E, \forall g, h \in G,\ g \cdot x = h \cdot x$ entails $g = h$
is regular if it is both transitive and free.

---

[8] There are two competing notations for the dihedral group associated to a polygon with n sides. In geometry the group is denoted D_n (as in the chapter on crystallogrpahy by Grenier and Ballou, while in algebra the same group is denoted by D_{2n} to indicate the number of elements (notation used here).

[9] We are actually dealing with a continuous action $\alpha : G \times \mathbb{R}^3 \to \mathbb{R}^3$ from a topological group G into a topological space V. It can be shown that any such continuous action entails an action β on the continuous functions defined on the topological space V via $(\beta_g f)(v) = f(\alpha_g^{-1} v)$.

In other words:
- A group action is effective (or faithful) if, apart from the identity of G, every element of G "moves" at least one element of E, or, equivalently, there is no element in $G\backslash\{e\}$ that would leave E invariant.
- An action is transitive if it is always possible to go from one element of E to another through the action of at least one element g of G.
- An action is free if the action of any two distinct group elements gives different results for any $x \in E$, i.e. if it differs for all elements $x \in E$. This statement is equivalent to saying that the only action that is allowed to possess fixed points, i.e. points not moved, is the action related to the neutral element: if $\exists x \in E$ such that $g \cdot x = x$ then $g = e$.
- An action is regular if for any two $x, y \in E$ there exists exactly one $g \in G$ such that $g \cdot x = y$. A regular action thus establishes a one to one relation between pairs of elements (x, y) in $E \times E$ with elements g in G.

Groups can act onto themselves. In this case the group structure allows to fully define the actions.

Let G be a group. Then G is canonically endowed with three actions

1) Left action:

$$\lambda : G \times G \longrightarrow G$$
$$(g, g') \longmapsto gg'$$

This action can be considered as trivial in the sense that it expresses nothing else but the fundamental relation defining the group as an algebraic structure.

2) Right action:

$$\rho : G \times G \longrightarrow G$$
$$(g, g') \longmapsto g'g^{-1}$$

This action is well-defined due to the existence of the inverse elements within G. It is a perfect example of how a group can act in a non-trivial way on a set, which in this case is its own carrier.

3) Conjugation action:

$$\chi : G \times G \longrightarrow G$$
$$(g, g') \longmapsto gg'g^{-1}$$

The conjugation action is a combination of left and right actions. We had encountered this action before in the context of equivalence classes. In the case of commutative groups left and right actions neutralize each other and the conjugation action maps every group element onto itself.

Exercise.
Proove that:
- They are all actions.
- The left and right actions λ and ρ are transitive.
- The conjugation action χ is not transitive, unless $G = \{e\}$.

We will now establish an important relation between group actions and homomorphisms of the symmetric group.

(6.1) Theorem.
Let G be a group and E a set. There exists a canonical bijection (symbolized by $\simeq$),

$$\mathrm{Hom}\,(G, S_E) \simeq \{\mathrm{Act} : G \times E \longrightarrow E\}$$

(between homomorphisms of G onto the permutation group of E, S_E, on one hand and the set of actions of G upon E on the other hand)

Proof.
We explicitly construct this bijection.

Let β be a group homomorphism from G to S_E. Then the image of $g \in G$ is a permutation (σ_g) of the elements $x \in E$. The expression $\beta(g)(x)$ is a well-defined function $f_g(x)$ mapping the elements of E onto themselves. We may, therefore, propose the mapping

$$\begin{aligned} \Phi : \mathrm{Hom}\,(G, S_E) &\longrightarrow \{\mathrm{Act} : G \times E \longrightarrow E\} \\ \beta &\longmapsto \left[\begin{array}{c} \alpha : G \times E \longrightarrow E \\ (g,x) \longmapsto f_g(x) := \beta(g)(x) \end{array}\right] \end{aligned}$$

We have to show that α is an action.

$$\begin{aligned} \alpha\left(g, \alpha(g',x)\right) &= \alpha\left(g, \beta(g')(x)\right) \\ &= \beta(g)\left(\beta(g')(x)\right) \\ &= \beta(g) \circ \beta(g')(x) \\ &\quad \text{and } \beta \text{ homomorphism} \Rightarrow \\ &= \beta(gg')(x) \\ &= \alpha(gg', x) \end{aligned}$$

Therefore, axiom (1) of the definition of a group action is fulfilled.
Moreover, $\alpha(e,x) = \beta(e)(x) = e_{S_E} x = x$. In consequence axiom (2) holds.
We, therefore, have demonstrated that α is an action.

Let us now consider the inverse direction. We propose

$$\begin{aligned} \Psi : \{\mathrm{Act} : G \times E \longrightarrow E\} &\longrightarrow \mathrm{Hom}\,(G, S_E) \\ \alpha &\longmapsto \left[\begin{array}{c} \beta : G \longrightarrow S_E \\ g \longmapsto \alpha(g,x) \end{array}\right] \end{aligned}$$

As α is an action β is a permutation (σ_g) of elements of E, which makes Ψ meaningful.
We have to show that β is indeed a homomorphism:
Let g, g' be two elements of G.

$$\begin{aligned} \beta(gg') &= \left[x \mapsto \alpha(gg', x)\right] \\ &= \left[x \mapsto \alpha\left(g, \alpha(g', x)\right)\right] \\ &= \left[x \mapsto \alpha(g', x) \mapsto \alpha\left(g, \alpha(g', x)\right)\right] \\ &= [x \mapsto \alpha(g, x)] \circ \left[x \mapsto \alpha(g', x)\right] \\ &= \beta(g)\beta(g') \end{aligned}$$

so β is a group homomorphism.
And Φ and Ψ are reciprocal bijections. □

(6.1) Corollary.
Every group is isomorphic to a subgroup of a group of permutations.
In particular, every finite subgroup is isomorphic to a subgroup of S_n provided n is correctly chosen.

To demonstrate the validity of this statement we consider the canonical left action λ of the group onto itself. This action corresponds to the inner law of the group. This inner law is homomorphic to the permutations in S_E. The group is thus isomorphic to a subgroup (the image of the homomorphism) of S_E.

This theorem is known under the name of **Cayley's theorem**, named in honor of Arthur Cayley. Its importance cannot be underestimated. It expresses the fact that everything to be learned about groups is basically contained in the groups of permutations. It equally implies that every finite group can be endowed with the canonical representation we have found for S_n. This is an extremely important result for the application of group theory to symmetry questions as those rely to a large extent on representations.

Example.

- Let us consider the quotient group $\mathbb{Z}/2\mathbb{Z}$ of the integer numbers modulo 2. It is a cyclic group of order 2 that partitions $\mathbb{Z}$ into even and odd numbers.
  Its carrier thus consists of the two elements $\{2\mathbb{Z}, 1+2\mathbb{Z}\}$.
  This group is isomorphic to the symmetric group of two elements S_2.
  The even numbers $2\mathbb{Z}$ correspond to the identity permutation in S_2 and the odd numbers $1+2\mathbb{Z}$ correspond to the interchange of two elements in S_2.
- Let us augment the complexity slightly by considering the quotient group $\mathbb{Z}/3\mathbb{Z}$ of the integer numbers modulo 3. Its carrier thus consists of the three elements $\{3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$.
  There is no symmetric group of order 3. We thus have to search among the subgroups of the symmetric groups. We find that $\mathbb{Z}/3\mathbb{Z}$ is isomorphic to a subgroup of the symmetric group of three elements S_3.
  The multiples of 3 given by $3\mathbb{Z}$ correspond to the identity permutation in S_3:

$$3\mathbb{Z} \longmapsto \sigma_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$

  The numbers with remainder 1 given by $1+3\mathbb{Z}$ can be identified with the cyclic change of elements in S_3:

$$1+3\mathbb{Z} \longmapsto \sigma_6 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

  The numbers with remainder 2 given by $2+3\mathbb{Z}$ have then to be identified with the inverse of σ_6, i.e. with the anti-cyclic change of elements in S_3:

$$2+3\mathbb{Z} \longmapsto \sigma_5 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

  We indeed verify that

$$(1+3\mathbb{Z}) \cdot (2+3\mathbb{Z}) = 3\mathbb{Z} = e$$

  In addition

$$(1+3\mathbb{Z}) \cdot (1+3\mathbb{Z}) = (2+3\mathbb{Z})$$

  in accordance with

$$\sigma_6 \cdot \sigma_6 = \sigma_5$$

  as required by the isomorphism.

With the help of the isomorphism we may immediately write down a three dimensional representation for $\mathbb{Z}/3\mathbb{Z}$ using the canonical representation of S_3:

$$\rho : \mathbb{Z}/3\mathbb{Z} \to GL_3(\mathbb{R}) :$$

$$3\mathbb{Z} \longmapsto A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$1 + 3\mathbb{Z} \longmapsto A_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$2 + 3\mathbb{Z} \longmapsto A_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

We indeed verify that $A_2 \cdot A_3 = A_1 = e$. A_2 is thus the inverse of A_3 (obtained by the inversion of columns and rows in the matrix). Equally, $A_2 \cdot A_2 = A_3$.
We conclude this example by reminding the reader that the subgroup $\sigma_1, \sigma_5, \sigma_6$ and thus the group $\mathbb{Z}/3\mathbb{Z}$ is isomorphic to the symmetry conserving rotations of an equilateral triangle in the plane.

We now turn our attention to the effect of group actions on subsets of E.

(6.3) Definition.
Let $\alpha : G \times E \longrightarrow E$ be a group action.
(1) A subset H of E is called **invariant** under α if the set $\{h' = g \cdot h : h \in H \text{ and } g \in G\}$ is identical to H.
(2) A subset H of E is called **fixed** under α if $\forall h \in H$ and $\forall g \in G$ it holds that $g \cdot h = h$.

Remark.
Any fixed subset is an invariant subset. The inverse is not necessarily true.

We now turn our attention to specific subsets created by the group action itself.

(6.4) Definition.
Let $\alpha : G \times E \to E$ be a group action of G on E. Take $x \in E$, then

$$\mathrm{Orb}(x) = \{g \cdot x\}_{g \in G}$$

is the **orbit** of x in E.

Remark.
- The orbit $\mathrm{Orb}(x)$ is thus a function that associates to every element $x \in E$ a subgroup of E, i.e. an element of the power set $\mathcal{P}(E)$.
- The orbit indicates the range of the action α when applied to x. This range is minimal if x is left invariant (fixed) by all elements $g \in G$. This is e.g. the case if G is the symmetry group of x. The range is maximum if the orbit of x coincides with E, i.e. if $\forall y \in E$, $\exists g \in G$ such that $g \cdot x = y$. This is necessarily the case for all transitive actions.
- The orbits are by definition invariant subsets of E.

- The group acts on these orbits by definition transitively as for every $y \in \mathrm{Orb}(x)$ we find at least one $g \in G$ such that $g \cdot x = y$.

Terminology.
The set of orbits $\{\mathrm{Orb}(x) : x \in E\}$ is called the quotient or equally the orbit space of the action and denoted by E/G.

We now show that a group action via its orbits partitions a set into equivalent classes. Two elements x and y of E are equivalent if and only if they belong to the same orbit of α, i.e. if there exists a $g \in G$ that moves x to y.

(6.1) Proposition.
Let $\alpha : G \times E \to E$ be a group action of G on the set E. Then the relation $\mathcal{R}_\alpha$ on E defined by

$$\mathcal{R}_\alpha(x, y) = T \Leftrightarrow \exists g \in G \text{ s.t. } g \cdot x = y \,[\Leftrightarrow y \in \mathrm{Orb}(x)]$$

is an equivalence relation and the orbits are the equivalence classes.

Proof.
We have to show that the relation is reflexive, symmetric and transitive.

1) Reflexivity: $\forall x \in E,\ \mathcal{R}_\alpha(x, x) = T$?
i.e. $\exists ? g$ s.t. $g \cdot x = x$: yes, with $g = e_G$.

2) Symmetry: $\forall x, y \in E,\ \mathcal{R}_\alpha(x, y) = T \overset{?}{\Rightarrow} \mathcal{R}_\alpha(y, x) = T$.
$\mathcal{R}_\alpha(x, y) = T \Rightarrow \exists g$ s.t. $y = g \cdot x$.
Therefore, $x = g^{-1} y$, i.e. $\mathcal{R}_\alpha(y, x) = T$.

3) Transitivity: Let there be x, y, z s.t. $\mathcal{R}_\alpha(x, y) = T$ and $\mathcal{R}_\alpha(y, z) = T$. Do we have $\mathcal{R}_\alpha(x, z) = T$?
$\mathcal{R}_\alpha(x, y) = T \Rightarrow \exists g$ s.t. $y = g \cdot x$
$\mathcal{R}_\alpha(y, z) = T \Rightarrow \exists g'$ s.t. $z = g' \cdot y$
so $z = g' \cdot (g \cdot x) = g' g \cdot x$, which means $\mathcal{R}_\alpha(x, z) = T$. □

(6.2) Corollary.
Every action $\alpha : G \times E \to E$ defines a partition of E, in orbits of the action.
In particular, it the action is transitive, the equivalence relation is trivial and defines only one class.

Terminology.
Let G be a group and

$$\begin{aligned} \chi : G \times G &\longrightarrow G \\ (g, g') &\longmapsto g g' g^{-1} \end{aligned}$$

the canonical conjugation action.
Then $\mathrm{Orb}(h) = \mathrm{Orb}_\chi(h)$ = conjugacy class of h.
The conjugacy class of e is reduced to e : $\mathrm{Orb}(e) = \{e\}$.
If the group is commutative, the conjugacy class of every element is reduced to itself.

Orbits are sets that indicate the potential of an action α to disperse x in E. We now define complementary sets that tell us about the resilience of an element $x \in E$ to be moved by the action α. It associates to every $x \in E$ the subset of G that leaves x invariant (or stable) under the action α.

(6.5) Definition.
Let $\alpha : G \times E \to E$ be a group action of G on the set E. Let $x \in E$.
Then

$$\mathrm{Stab}_\alpha(x) = \{g \in G \text{ s.t. } g \cdot x = x\}$$

is the **stabilizer** of x.

(6.2) Proposition.

$$\forall x \in E,\ \mathrm{Stab}_\alpha(x) \text{ is a subgroup of } G.$$

In addition,

$$\mathrm{Orb}_\alpha(x) \simeq \{\text{right cosets or left cosets of } G \text{ modulo } \mathrm{Stab}_\alpha(x)\}\,.$$

This theorem is known as the orbit-stabilizer theorem as it establishes a close relation between the orbits and the stabilizer of an element $x \in E$ (see Fig. 8).

Proof.
(1) Is $\mathrm{Stab}(x)$ a subgroup of G?
Let $\alpha : G \times E \to E$ be an action. Let $x \in E$.
Indeed, $e \cdot x = x$. Therefore, $x \in \mathrm{Stab}(x) \neq \emptyset$.
Let $a, b \in \mathrm{Stab}(x)$: $b \cdot x = x$.
Then $b^{-1}b \cdot x = e \cdot x = x$ and also, $b^{-1}b \cdot x = b^{-1} \cdot x$ because $b \in \mathrm{Stab}(x)$.
Therefore $b^{-1} \cdot x = x$, i.e. $b^{-1} \in \mathrm{Stab}(x)$.
So $ab^{-1} \cdot x = a \cdot (b^{-1} \cdot x) = a \cdot x = x$, which shows that $ab^{-1} \in \mathrm{Stab}(x)$.
It follows that $\mathrm{Stab}(x)$ is is indeed a subgroup of G.

(2) Let us show that $G/\mathrm{Stab}(x) \simeq \mathrm{Orb}(x)$.
We note $\mathrm{Stab}(x) = S$ for the sake of simplicity. We define for every x the application

$$\begin{aligned} \alpha_x : G/S &\longrightarrow \mathrm{Orb}(x) \\ gS &\longmapsto g \cdot x = \alpha(g, x) \end{aligned}$$

from the cosets of G modulo S into the orbits of x under the action α.
We first have to show that this definition is unambiguous!
Let h be another representative of the coset gS.
Then we have $hS = gS$, which means that $h^{-1}g \in S$.
Because $h^{-1}g \in S$, we have $(h^{-1}g) \cdot x = x$ by definition of the stabilizer S.
Consequently, $h \cdot x = h \cdot ((h^{-1}g) \cdot x) = hh^{-1}g \cdot x = g \cdot x$, i.e., $h \cdot x = g \cdot x$.
The application $G/S \underset{\alpha_x}{\longrightarrow} \mathrm{Orb}(x)$ is thus well defined.
α_x is surjective:
$y \in \mathrm{Orb}(x) \Leftrightarrow y = g \cdot x$
$\Rightarrow \exists g \in G$ such that $y = \alpha_x(gS)$.

α_x is injective:
gS and hS two elements of G/S, such that $g \cdot x = h \cdot x$.
Then $h^{-1}g \cdot x = h^{-1}h \cdot x = e \cdot x = x$, so $h^{-1}g \in S \Leftrightarrow gS = hS$.

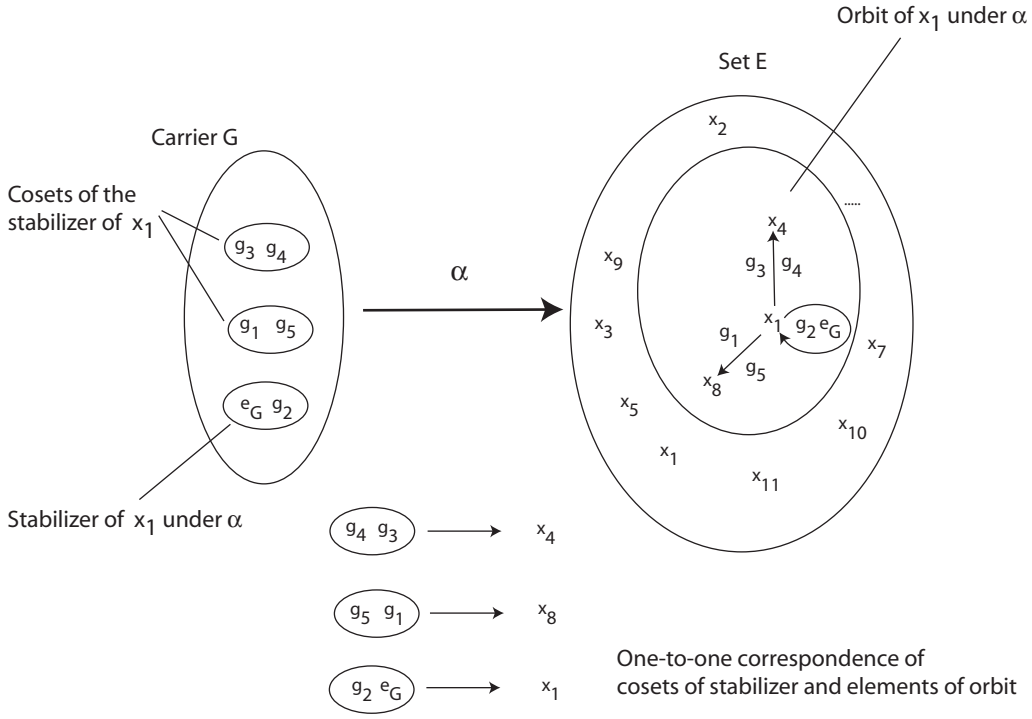


Figure 8. Schematic representation of an orbit and a stabilizer. The group G acts on the set E via the group action α. The element $x_1 \in E$ is left invariant by the action of the group elements e_g and g_2. The set $\{e_g, g_2\}$ is thus the stabilizer or little group of x_1. The orbit of x_1 is given by the set of points that x_1 is moved to under the action of α. The orbit-stabilizer theorem establishes a one-to-one correspondence between the cosets of the stabilizer and the elements of the orbit.

By showing that $G/\mathrm{Stab}(x) \simeq \mathrm{Orb}(x)$, we have demonstrated that there exists a biunivoque correspondence between every element of an orbit and an equivalence class modulo the stabilizer. This is precisely what we had to prove. □

Terminology.
The stabilizer subgroup is equally called the isotropy or little group of x.

Remark.
The stabilizer is not necessarily a normal subgroup of G.

(6.3) Proposition.
Let $\alpha : G \times E \to E$ be a group action of G on E.
Let $x \in E$ and $\mathrm{Orb}(x)$ its orbit, and $y \in \mathrm{Orb}(x)$.
Then $\mathrm{Stab}(x)$ and $\mathrm{Stab}(y)$ are conjugate.

Proof.
Let $S_x = \mathrm{Stab}(x)$ and $S_y = \mathrm{Stab}(y)$. We want to build an inner automorphism that "bridges" S_x to S_y (then, they will be conjugate).

$$\begin{aligned} S_x &\xrightarrow{\mathrm{Int}_h} S_y \\ g &\longmapsto hgh^{-1} \end{aligned}$$

The difficulty is to find the "right" h.
Because $y \in \mathrm{Orb}(x)$, $\exists h$ such that $y = h \cdot x$. Let g be an element of S_x, then $g \cdot x = x$. Do we have $hgh^{-1} \in S_y$? (If so, then we have found an h that fits)

$$\begin{aligned} hgh^{-1} \cdot y &= hgh^{-1} \cdot (hx) \\ &= hg \cdot x \\ &= h \cdot x = y \end{aligned}$$

And along the same spirit,

$$\begin{aligned} S_y &\xrightarrow{\mathrm{Int}_{h^{-1}}} S_x \\ g &\longmapsto h^{-1}gh \end{aligned}$$

The two stabilizers are conjugate. □

(6.3) Corollary.
If the action is transitive, then all stabilizers are conjugate.
(Indeed, if α is transitive, we only have one orbit)

7. CONCLUSION

This short introduction to group theory aimed at exposing the notion of group structure, the way groups can be mapped one onto another, and how groups can operate on ensembles. Although kept at a rather simple level, this exposure is enough to prepare to the next step, i.e linear group representations. Although the concept of representation of a group can be presented in a formal way, one should keep in mind that from the physical point of view, the most common usage of group representations is through an algebra of matrices. In physics, matrices are related to mappings between vector spaces or Hilbert spaces, and are most often endomorphisms, i.e mapping of a vector space onto itself. When it comes to symmetry, the idea is to translate the operation the physicist is dealing with into an algebraic object that can be worked out with the tool set of group theory. Without the notion of group theory, one is most often left with clever tricks or observations. For instance, observing that the dynamics of a spring can be decompose into a symmetric and an antisymmetric component, or that Fourier transforming an operator can sometimes diagonalize it. Actually, there are group arguments in both cases, that are much deeper than it seems. In order to use the full power of group theory, one has to properly construct how an abstract group can act onto a vector space, i.e, as will be shown hereafter, that it is possible to construct an action of an abstract group onto the linear group of a given vector space. When done, this correspondence will allow to map completely the whole set of the abstract group properties onto the vector space. Although those remarks might sound like a little bit abstract here, one should keep in mind that the two examples given above are nothing but the application of a *projector* onto functions or operators, and that these *projectors* can be constructed *systematically*, given an abstract group, and almost *independently* of the vector space it is acting on.

Put another way, when it comes to symmetry, you have two alternatives. First, if you are clever enough, you find out by yourself how the symmetries of your problem can be translated into the formalism you are using and how they can simplify and identify properly the physical properties:

symmetry of an order parameter, quantum numbers, etc. Or, if you are like the authors, not clever at all, identify what is the abstract group behind all the symmetries, use all the mechanics and systematics of group theory and group actions, which will find for yourself everything that can be found.

References

[1] Elements de mathématiques, Nicolas Bourbaki, Springer, Heidelberg.
[2] Group Theory and Its Application to Physical Problems, Morton Hamermesh, Dover Books on Physics (1989).