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.

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.

(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 $b = c$. □

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.

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.

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

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

$\Leftrightarrow$ the diagram:

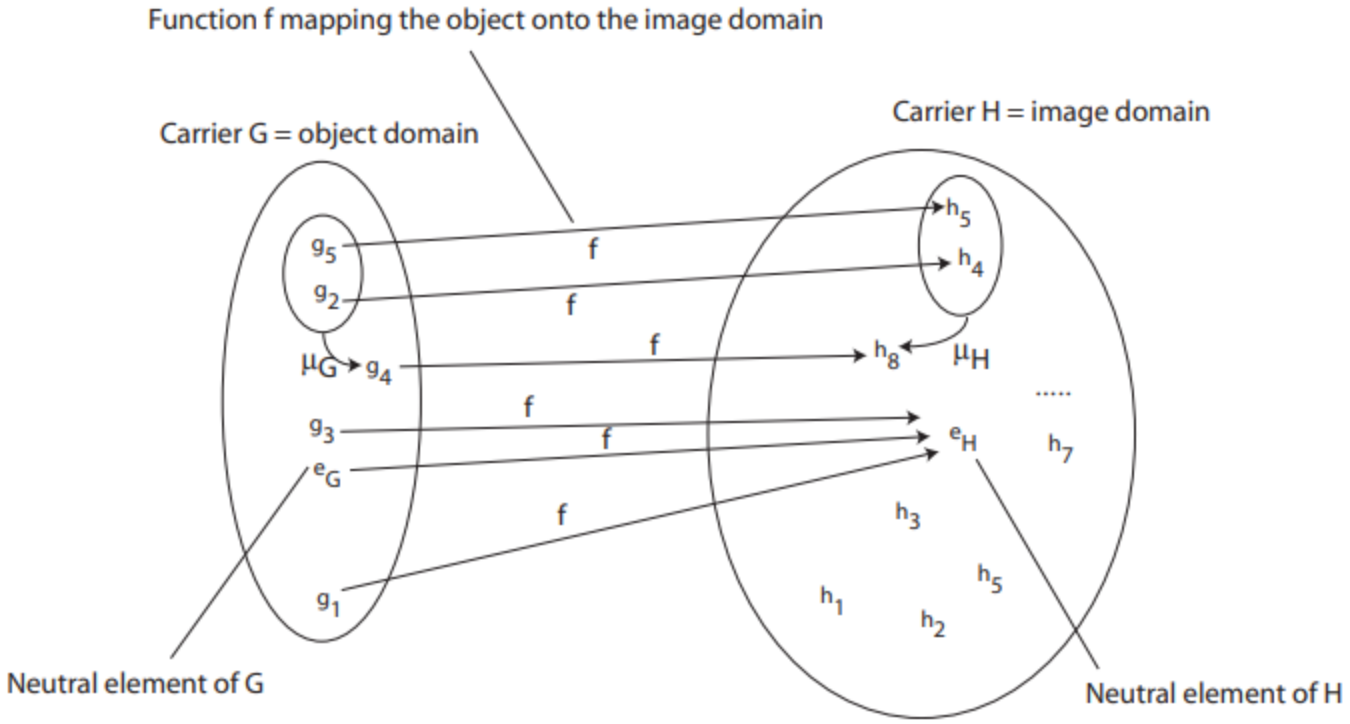
$$\begin{array}{ccc} G_1 \times G_1 & \xrightarrow{\mu_1} & G_1 \\ \downarrow{\scriptstyle f\times f} & \bigcirc & \downarrow{\scriptstyle f} \\ G_2 \times G_2 & \xrightarrow{\mu_2} & G_2 \end{array}$$

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.


Function f mapping the object onto the image domain
Carrier G = object domain
Carrier H = image domain
g5
g2
μG
g4
g3
eG
g1
f
f
f
f
f
f
h5
h4
h8
μH
.....
eH
h7
h3
h5
h1
h2
Neutral element of G
Neutral element of H

(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. □

A group is said to be "abelian" if $x * y = y * x$ for every $x, y \in G$. All of the examples above are abelian groups. The set of symmetries of an equilateral triangle forms a group of size 6 under composition of symmetries. It is the smallest group which is NOT abelian.

Definition 2. *A* **RING** *is a set R which is CLOSED under two operations $+$ and $\times$ and satisfying the following properties:*

(1) *R is an abelian group under $+$.*
(2) *Associativity of $\times$ – For every $a, b, c \in R$,*

$$a \times (b \times c) = (a \times b) \times c$$

(3) *Distributive Properties – For every $a, b, c \in R$ the following identities hold:*

$$a \times (b + c) = (a \times b) + (a \times c)$$

and

$$(b + c) \times a = b \times a + c \times a.$$

Examples:

(1) Both the examples $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ from before are also RINGS. Note that we don't require multiplicative inverses.
(2) $\mathbb{Z}[x]$, fancy notation for all polynomials with integer coefficients. Multiplication and addition is the usual multiplication and addition of polynomials.

Definition 3. *A* **FIELD** *is a set F which is closed under two operations $+$ and $\times$ such that*

(1) *F is an abelian group under $+$ and*
(2) *$F - \{0\}$ (the set F without the additive identity 0) is an abelian group under $\times$.*

Examples: $\mathbb{Z}/p\mathbb{Z}$ is a field, since $\mathbb{Z}/p\mathbb{Z}$ is an additive group and $(\mathbb{Z}/p\mathbb{Z}) - \{0\} = (\mathbb{Z}/p\mathbb{Z})^\times$ is a group under multiplication. Sometimes when we (or Cox) want to emphasize that $\mathbb{Z}/p\mathbb{Z}$ is a field, we use the notation $\mathbb{F}_p$. Other examples: $\mathbb{R}$, the set of real numbers, and $\mathbb{C}$, the set of complex numbers are both infinite fields. So is $\mathbb{Q}$, the set of rational numbers, but not $\mathbb{Z}$, the integers. (What fails?)