Abstract Algebra
A Short Summary

Basilio Bona

DAUIN – Politecnico di Torino

July 2009
A groupoid \( \{G; \circ\} \) is one of the most general algebraic structures. It consists of a set \( G \) of elements and a binary operator \( \circ \), that in general is neither associative nor commutative, but only closed wrt elements of \( G \) if \( a, b \in G \), then also \( a \circ b = c \in G \).

The operator \( \circ \) is not a “sum” or a “product”, since it may represent a very general operation, like e.g., a string concatenation, the maximum common divisor, a projection on a subspace, etc.

The operator \( \circ \) may be only a partial operator, i.e., the totality property does not necessarily holds.

When \( \circ \) is amenable to a sum the groupoid is said to be additive, while if \( \circ \) is amenable to a sum the groupoid is said to be multiplicative.
A **semigroup** is an associative groupoid, i.e., a groupoid \( \{ G; \circ \} \) where \( \circ \) is associative

if \( a, b, c \in G \), then \( a \circ (b \circ c) = (a \circ b) \circ c \)

A *neutral element* is not required, as for the monoid, as well as a *unit* (unitary) element, as for the group.
A monoid is a semigroup \( \{M; \circ, u\} \) with a neutral element wrt to \( \circ \). The neutral element \( u \) is also called identity element or unit element

\[
\forall a \in M, \quad a \circ u = u \circ a = a.
\]

Often the neutral element is indicated with the symbol 0 if the operator \( \circ \) is amenable to a sum, or with the symbol 1 if the operator \( \circ \) is amenable to a product.

No inverse element is assumed.
A group $G$ is an algebraic structure defined by the monoid axioms plus the existence of an inverse element.

This structure makes a group sufficiently rich to be of some interest in mathematical physics and engineering (e.g., the rotation group $SO(3)$).

Hence a group is a monoid $\{G; \circ, u, a^{-1}\}$, with an inverse element $a^{-1}$:

$$\forall a \in G \; \exists a^{-1}, \; \text{such that} \; a \circ a^{-1} = a^{-1} \circ a = u.$$ 

In particular,

- if $a \circ a^{-1} = u$, the element is called right inverse,
- if $a^{-1} \circ a = u$, the element is called left inverse.

If the operator $\circ$ is the sum, the inverse of $a$ is commonly indicated as $-a$; if $\circ$ is the product, the inverse is indicated as $a^{-1}$.

The presence of an inverse requires that the group should have at least one element.
A group $G$ is called *commutative* or *abelian* if the operator $\circ$ arguments commute

$$\forall a, b \in G \quad a \circ b = b \circ a$$

In this case, right and left inverse coincide.

A *semigroup* differs from a group in that for each of its elements there may not exist an inverse; further, there may not exist an identity element.
Examples

- The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, of integer, rational, real, and complex numbers are **commutative** groups wrt the sum operator, $\circ \equiv +$.

- The sets $\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$ of nonzero rational real and complex numbers form a **commutative** group wrt to the product operator, $\circ \equiv \times$.

- The set $GL(n, \mathbb{R})$ of $n \times n$ invertible matrices, form a **non-commutative** group wrt to the usual matrix product.

- The set $S_X$ of all bi-injective transformations of a set $X$ in itself, form a **non-commutative** group wrt to the operator $\circ$ that composes the transformations, i.e., $(f \circ g)(x) = f(g(x))$.

- The rigid rotations in 3D space form a **non-commutative** group wrt the matrix product. This group is called **Special Orthonormal group of dimension 3**

$$SO(3) = \left\{ R \in \mathbb{R}^{3 \times 3} \mid R^T R = I, \det R = +1 \right\}$$
<table>
<thead>
<tr>
<th>Structure</th>
<th>Totality</th>
<th>Associativity</th>
<th>Identity</th>
<th>Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Monoid</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Semigroup</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Loop</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Quasigroup</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Magma</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Groupoid</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Category</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

Properties of the group-like structures [Wikipedia].
A ring $\mathcal{A}$ is a system $\{\mathcal{A}; +, \cdot\}$, i.e., a set of elements $a \in \mathcal{A}$, together with two operations $+$ and $\cdot$, called sum (or addition) and product (or multiplication), satisfying the following two axioms:

1. $\{\mathcal{A}, +\}$ is a commutative group with neutral element 0, called ring additive group.
2. $\{\mathcal{A}, \cdot\}$ is a semigroup.

A division ring, also called a skew field, is a ring in which division is possible. More formally, a ring with $0 \neq 1$ is a division ring if every non-zero element $a$ has a multiplicative inverse (i.e., an element $x$ with $ax = xa = 1$). Division rings differ from fields only in that their multiplication is not required to be commutative.

Stated differently, a ring is a division ring if and only if the group of units is the set of all non-zero elements.

All fields are division rings; more interesting examples are the non-commutative division rings. The best known example is the ring of quaternions $\mathbb{H}$. 
Properties

- **associativity wrt sum:**
  \[ \forall a, b, c \in A \quad (a + b) + c = a + (b + c) \]

- **commutativity wrt sum:**
  \[ \forall a, b \in A \quad a + b = b + a \]

- **existence of neutral element wrt sum:**
  \[ \exists 0 \in A \rightarrow \forall a \in A \quad 0 + a = a + 0 = a \]

- **existence of inverse element wrt sum:**
  \[ \forall a \in A \rightarrow \exists (-a) \in A, a + (-a) = (-a) + a = 0 \]

- **associativity wrt product:**
  \[ \forall a, b, c \in A \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c \]

- **distributivity of product wrt sum:**
  \[ \forall a, b, c \in A \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]

A ring contains at least one element.
Properties **not** possessed by rings:

1. the existence of a neutral element wrt product is not required. If it exists it is called *unit* or *unity*;
2. no axiom on quotients is required; in particular if \( A \) has a unit, it is not required that a non-null element \( a \neq 0 \) has an inverse (left, right or bilateral);
3. no commutative property wrt product is assumed;
4. no product cancellation law is assumed: the existence of ring with elements \( a \neq 0 \) such that \( a \cdot b = 0 \), or \( b \cdot a = 0 \) for some \( b \neq 0 \); this implies that, if \( a \cdot b = a \cdot c \), not necessarily \( b = c \). \( a \) is said to be a *left divisor of zero*, since \( b = a^{-1} \cdot 0 \), and \( b \) *right divisor of zero*, since \( a = 0 \cdot b^{-1} \).

Product cancellation law establishes that, given \( b \neq 0 \), if \( a \cdot b = 0 \), then \( a = 0 \).
Examples of rings:

1. The familiar matrix algebra, where in general the commutativity property does not hold, where non invertible elements exist, and where it is possible to have non zero elements whose product is null. Moreover it is known that, in general, $AB = AC$ does not imply $B = C$. Therefore the set ad square matrices $M \in \mathbb{R}^{n \times n}$, with $n \geq 2$, forms a non commutative ring with divisors of the zero.

2. The integer numbers set $\mathbb{Z}$ is a ring $\{\mathbb{Z}, +, \cdot\}$ with identity; however it is not a division ring.

3. Let $m$ be an integer and $m\mathbb{Z} = \{n \in \mathbb{Z} \mid m \text{ divides } n\}$ be the set of integer multiple of $m$. Then $\{m\mathbb{Z}, +, \cdot\}$ is a ring, but devoid of the identity unless $m = \pm 1$. 
If to the axioms of a ring, one adds the existence of an inverse element for the product, a **field** is obtained.

A field $\mathcal{F}$ is a system $\{\mathcal{F}; +, \cdot\}$ of elements $\alpha \in \mathcal{F}$ and two operations $+, \cdot$ called **sum** (or **addition**) and **product** (or **multiplication**), satisfying the following three axioms:

1. $\{\mathcal{F}, +\}$ is a commutative group with neutral element $0$, called **field additive group**.
2. $\{\mathcal{F}^*, \cdot\}$ is a commutative group with unit $u$ or $1$, where $\mathcal{F}^* = \mathcal{F} - \{0\}$. $\{\mathcal{F}^*, \cdot\}$ is called **field multiplicative group**.
3. Operator $\cdot$ has distributive property wrt $+$, i.e., given $\alpha, \beta, \gamma \in \mathcal{F}$:

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

(already included in the ring axioms).
An alternative definition is the following:

A **field** is a division ring (or a skew field) with a commutative multiplicative group.

Observe that a field is a commutative division ring both for the sum and for the product.

The inverse wrt the sum is indicated by \(-\alpha\), while the inverse wrt the product is indicated by \(\alpha^{-1}\).
A commutator of two elements $a$ and $b$ of a ring or an associative algebra is defined by

$$[a, b] := a \cdot b - b \cdot a$$

where $a \cdot b$ is the product defined on the ring.

The commutator is zero if and only if $a$ and $b$ commute, i.e., $a \cdot b = b \cdot a$.

By using the commutator as a Lie bracket, every associative algebra can be turned into a Lie algebra (see below).

**Properties:**

1. $[a, a] = 0$
2. $[a, b] = -[b, a]$
3. Jacoby identity: $[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$
The word *algebra* derives from the title “Hisab al-jabr w’al-muqabala” of a book that for the first time used algebraic methods, whose author was the Persian mathematician Muhammed ibn Musa Al-Khwarizmi (circa 780-850), whose deformed name gave origin to the word *algorithm*.

In the modern use the word takes different meanings:

1. **Algebra** as the subject taught in the secondary schools and universities, distinct from geometry, that introduces polynomial equations, one- or multi-variable functions, maxima and minima, etc. It is also called elementary algebra or arithmetics.

2. **Algebra** as the study of numbers and their properties, adopting the concepts of group, ring, invariant theory, etc. It is also called abstract algebra.

3. **Algebra** to indicate a particular formal structure or system governing a set of elements: in this sense algebra is a branch of mathematics concerning the study of structure, relation, and quantity.

4. **Algebraic geometry**, algebra of a vector space defined on a field with a product operator, as seen above.
Some examples:

- **Associative algebras**: the algebra of all \( n \times n \) matrices over the field (or commutative ring) \( F \). Here the multiplication is ordinary matrix multiplication.

- **Non-associative algebras**: Lie algebras, for which we require \( xx = 0 \) and the Jacobi identity \((xy)z + (yz)x + (zx)y = 0\). For these algebras the product is called the Lie bracket and is conventionally written \([x,y]\) instead of \(xy\). Examples include: Euclidean space \( \mathbb{R}^3 \) with multiplication given by the vector cross product (with \( F \) the field \( \mathbb{R} \) of real numbers); algebras of vector fields on a differentiable manifold (if \( F \) is \( \mathbb{R} \) or the complex numbers \( \mathbb{C} \)) or an algebraic variety (for general \( F \)); every associative algebra gives rise to a Lie algebra by using the commutator as Lie bracket.
A morphism is an abstraction derived from structure-preserving mappings between two mathematical structures.

Morphisms are not necessarily functions, and objects over which morphisms are defined are not necessarily sets. Instead, a morphism is often thought of as an arrow (i.e., a relation) linking an object called the domain to another object called the codomain. The composition of morphisms is indicated with $\circ$.

Morphisms satisfy two axioms

1. **Identity**: for every abstract structure $X$, there exists a morphism $\mathbb{I}_X : X \rightarrow X$ called the identity morphism on $X$, such that for every morphism $f : A \rightarrow B$ we have $\mathbb{I}_B \circ f = f = f \circ \mathbb{I}_A$.

2. **Associativity**: $h \circ (g \circ \varphi) = (h \circ g) \circ \varphi$ whenever the operations are defined.
Isomorphisms are studied in mathematics in order to extend insights from one phenomenon to others: if two objects are isomorphic, then any property which is preserved by an isomorphism and which is true of one of the objects is also true of the other. If an isomorphism can be found from a relatively unknown part of mathematics into some well studied division of mathematics, where many theorems are already proved, and many methods are already available to find answers, then the function can be used to map whole problems out of unfamiliar territory over to "solid ground" where the problem is easier to understand and work with.

\( \varphi : X \to Y \) is called an **isomorphism** if there exists a morphism \( \varphi' : Y \to X \) such that

\[
\varphi \circ \varphi' = \mathbb{I}_Y \quad \text{and} \quad \varphi' \circ \varphi = \mathbb{I}_X
\]
An endomorphism is a morphism from a mathematical structure to itself

\[ \varphi : X \rightarrow X \]
In abstract algebra, a **homomorphism** is a structure-preserving map between two algebraic structures (such as groups, rings, or vector spaces). The word homomorphism comes from the Greek language: ὁμός (homos) meaning “same” and ὀρφή (morphe) meaning “shape”. Note the similar root word ὀμοιός (homoios), meaning “similar,” which is found in another mathematical concept, namely homeomorphisms.

A group homomorphism indeed preserves group structure, because it not only preserves products, but also the identity and inverses.

Thus the image \( \varphi(G) \) is of similar form to \( G \), but we say that \( G' \) is isomorphic (of the same form) to \( G \) only when the map \( \varphi \) is 1-to-1 and onto (in which case we call \( \varphi \) an **isomorphism**).

In general, \( \varphi(G) \) is only a shadow of \( G \), because many elements of \( G \) may map to the same element of \( G' \).

The case furthest from isomorphism is that in which \( \varphi \) sends all elements of \( G \) to 1.
An **automorphism** is an isomorphism of a system of objects onto itself.

\[
\begin{align*}
\text{AUTOMORPHISM} & \quad \equiv \quad \text{ISOMORPHISM} \\
\downarrow & \quad \downarrow \\
\text{ENDOMORPHISM} & \quad \equiv \quad \text{HOMOMORPHISM}
\end{align*}
\]

**Figure:** Hierarchy of morphisms.
A **diffeomorphism** is an isomorphism in the *category* of smooth manifolds. It is an invertible function that maps one differentiable manifold into another (of the same dimension), such that both the function and its inverse are smooth.

Given two manifolds $M$ and $N$, a bijective map $\varphi$ from $M$ to $N$ is called a diffeomorphism if both

$$\varphi : M \rightarrow N \quad \text{and its inverse} \quad \varphi^{-1} : N \rightarrow M$$

are differentiable.

If $\varphi$ and $\varphi^{-1}$ are $r$ times continuously differentiable, $f$ is called a $C^r$-diffeomorphism. Two manifolds $M$ and $N$ are diffeomorphic ($M \simeq N$) if there is a smooth bijective function $\varphi$ from $M$ to $N$ with smooth inverse. They are $C^r$ diffeomorphic if there is an $r$ times continuously differentiable bijective function between them, whose inverse is also $r$ times continuously differentiable.
Figure: A diffeomorphism from a square onto itself.
In the mathematical field of topology, a **homeomorphism** (from Greek ὁμοιός (homoios), meaning “similar”) or topological isomorphism is a bicontinuous function between two topological spaces.

Homeomorphisms are the isomorphisms in the category of topological spaces – that is, they are the mappings which preserve all the topological properties of a given space.

Two spaces with a homeomorphism between them are called homeomorphic, and from a topological viewpoint they are the same.
In mathematics, **holomorphic functions** are the central object of study of complex analysis; they are functions defined on an open subset of the complex number plane $\mathbb{C}$ with values in $\mathbb{C}$ that are complex-differentiable at every point.

This is a much stronger condition than real differentiability and implies that the function is infinitely often differentiable and can be described by its Taylor series.