

Abstract Algebra Overview I (H.1)

20160621

Copyright (c) 2016 Young W. Lim.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Algebraic Structure

In mathematics, and more specifically in abstract algebra, the term **algebraic structure** generally refers to a set (called **carrier set** or **underlying set**) with one or more finitary operations defined on it that satisfies a list of axioms.^[1]

Examples of algebraic structures include groups, rings, fields, and lattices. More complex structures can be defined by introducing multiple operations, different underlying sets, or by altering the defining axioms. Examples of more complex algebraic structures include vector spaces, modules and algebras.

(groups
rings
fields
lattices

(Vector space
modules
algebras

Set, Group, Ring, Field

A **set** is a collection of unique elements. The definition of a specific set determines which elements are members of the set. Elements not specifically defined as members of a set are not in the set.

A **group** is an algebraic system consisting of **a set**, **an identity element** for each operation, **one** operation and **its inverse operation**.

A **ring** is an algebraic system consisting of **a set**, **an identity element** for each operation, **two** operations and **the inverse operation of the first operation**.

A **field** is an algebraic system consisting of **a set**, **an identity element** for each operation, **two** operations and **their respective inverse operations**.

http://www.csee.umbc.edu/portal/help/theory/group_def.shtml

Group Definition

A group is a **set**, G , together with an **operation** \cdot (called the *group law* of G) that combines any two **elements** a and b to form another element, denoted $a \cdot b$ or ab . To qualify as a group, the set and operation, (G, \cdot) , must satisfy four requirements known as the **group axioms** [5]

Closure

For all a, b in G , the result of the operation, $a \cdot b$, is also in G . [6]

⑥ Associativity

For all a, b and c in G , $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Identity element

There exists an element e in G , such that for every element a in G , the equation $e \cdot a = a \cdot e = a$ holds. Such an element is unique (see below), and thus one speaks of *the* identity element.

Inverse element

For each a in G , there exists an element b in G , commonly denoted a^{-1} (or $-a$, if the operation is denoted "+"), such that $a \cdot b = b \cdot a = e$, where e is the identity element.

[T]he axioms for a group are short and natural... Yet somehow hidden behind these axioms is the **monster simple group**, a huge and extraordinary mathematical object, which appears to rely on numerous bizarre coincidences to exist. The axioms for groups give no obvious hint that anything like this exists.

Richard Borcherds in *Mathematicians: An Outer View of the Inner World* [4]

Abelian group

From Wikipedia, the free encyclopedia

For the group described by the archaic use of the related term "Abelian group".

In abstract algebra, an **abelian group**, also called a **commutative group**, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written (the axiom of commutativity). Abelian groups generalize the arithmetic of addition of integers. They are named after Niels Henrik Abel.^[1]

A **group** is an algebraic system consisting of a set, an **identity element** for each operation, **one** operation and **its inverse operation**.

Abelian Group Definition

An abelian group is a **set**, A , together with an **operation** \bullet that combines any two **elements** a and b to form another element denoted $a \bullet b$. The symbol \bullet is a general placeholder for a concretely given operation. To qualify as an abelian group, the set and operation, (A, \bullet) , must satisfy five requirements known as the *abelian group axioms*:

Closure

For all a, b in A , the result of the operation $a \bullet b$ is also in A .

⑥ Associativity

For all a, b and c in A , the equation $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ holds.

Identity element

There exists an element e in A , such that for all elements a in A , the equation $e \bullet a = a \bullet e = a$ holds.

Inverse element

For each a in A , there exists an element b in A such that $a \bullet b = b \bullet a = e$, where e is the identity element.

★ Commutativity

For all a, b in A , $a \bullet b = b \bullet a$.

More compactly, an abelian group is a **commutative group**. A group in which the group operation is not commutative is called a "non-abelian group" or "non-commutative group".

Orthogonal Groups

In mathematics, the **orthogonal group** in dimension n , denoted $O(n)$, is the group of distance-preserving transformations of a Euclidean space of dimension n that preserve a fixed point, where the group operation is given by composing transformations. Equivalently, it is the group of $n \times n$ orthogonal matrices, where the group operation is given by matrix multiplication, and an orthogonal matrix is a real matrix whose inverse equals its transpose.

The determinant of an orthogonal matrix being either 1 or -1 , an important subgroup of $O(n)$ is the **special orthogonal group**, denoted $SO(n)$, of the orthogonal matrices of determinant 1. This group is also called the **rotation group**, because, in dimensions 2 and 3, its elements are the usual rotations around a point (in dimension 2) or a line (in dimension 3). In low dimension, these groups have been widely studied, see $SO(2)$, $SO(3)$ and $SO(4)$.

Ring Definition

A **ring** is a set R equipped with binary operations^[1] $+$ and \cdot satisfying the following three sets of axioms, called the ring axioms^{[2][3][4]}

1. R is an abelian group under addition, meaning that

- $(a + b) + c = a + (b + c)$ for all a, b, c in R ($+$ is associative).
- $a + b = b + a$ for all a, b in R ($+$ is commutative).
- There is an element 0 in R such that $a + 0 = a$ for all a in R (0 is the additive identity).
- For each a in R there exists $-a$ in R such that $a + (-a) = 0$ ($-a$ is the additive inverse of a).

2. R is a monoid under multiplication, meaning that:

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in R (\cdot is associative).
- There is an element 1 in R such that $a \cdot 1 = a$ and $1 \cdot a = a$ for all a in R (1 is the multiplicative identity).^[5]

3. Multiplication is distributive with respect to addition:

- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all a, b, c in R (left distributivity).
- $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all a, b, c in R (right distributivity).

A **ring** is an algebraic system consisting of a **set**, an **identity element** for each operation, **two** operations and the inverse operation of the first operation.

Monoid

In abstract algebra, a branch of mathematics, a **monoid** is an algebraic structure with a single associative binary operation and an identity element. Monoids are studied in semigroup theory as they are semigroups with identity. Monoids occur in several branches of mathematics; for instance, they can be regarded as **categories** with a single **object**. Thus, they capture the idea of **function composition** within a set. Monoids are also commonly used in **computer science**, both in its foundational aspects and in practical programming. The set of **strings** built from a given set of **characters** is a **free monoid**. The **transition monoid** and **syntactic monoid** are used in describing **finite state machines**, whereas **trace monoids** and **history monoids** provide a foundation for **process calculi** and **concurrent computing**. Some of the more important results in the study of monoids are the **Krohn-Rhodes theorem** and the **star height problem**. The history of monoids, as well as a discussion of additional general properties, are found in the article on **semigroups**.

Monoid Definition

Definition [edit]

Suppose that S is a [set](#) and \cdot is some [binary operation](#) $S \times S \rightarrow S$, then S with \cdot is a **monoid** if it satisfies the following two axioms:

Associativity

For all a, b and c in S , the equation $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ holds.

Identity element

There exists an element e in S such that for every element a in S , the equations $e \cdot a = a \cdot e = a$ hold.

In other words, a monoid is a [semigroup with an identity element](#). It can also be thought of as a [magma](#) with associativity and identity. The identity element of a monoid is unique.^[1] A [monoid in which each element has an inverse](#) is a [group](#).

Depending on the context, the symbol for the binary operation may be omitted, so that the operation is denoted by juxtaposition; for example, the monoid axioms may be written $(ab)c = a(bc)$ and $ea = ae = a$. This notation does not imply that it is numbers being multiplied.

In mathematics, a **semigroup** is an algebraic structure consisting of a set together with an associative binary operation. The binary operation of a semigroup is most often denoted multiplicatively: $x \cdot y$, or simply xy , denotes the result of applying the semigroup operation to the ordered pair (x, y) . Associativity is formally expressed as that $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all x, y and z in the semigroup.

The name "semigroup" originates in the fact that a semigroup generalizes a group by preserving only associativity and closure under the binary operation from the axioms defining a group.^[note 1] From the opposite point of view (of adding rather than removing axioms), a semigroup is an associative magma. As in the case of groups or magmas, the semigroup operation need not be commutative, so $x \cdot y$ is not necessarily equal to $y \cdot x$; a typical example of associative but non-commutative operation is matrix multiplication. If the semigroup operation is commutative, then the semigroup is called a *commutative semigroup* or (less often than in the analogous case of groups) it may be called an *abelian semigroup*.

A **monoid** is an algebraic structure intermediate between groups and semigroups, and is a semigroup having an **identity element**, thus obeying all but one of the axioms of a group; existence of inverses is not required of a monoid. A natural example is **strings** with **concatenation** as the binary operation, and the empty string as the identity element. Restricting to non-empty **strings** gives an example of a semigroup that is not a monoid. Positive **integers** with addition form a commutative semigroup that is not a monoid. Whereas the non-negative **integers** do form a monoid. A semigroup without an identity element can be easily turned into a monoid by just adding an identity element. Consequently, monoids are studied in the theory of semigroups rather than in group theory. Semigroups should not be confused with **quasigroups**, which are a generalization of groups in a different direction; the operation in a quasigroup need not be associative but quasigroups **preserve from groups** a notion of **division**. Division in semigroups (or in monoids) is not possible in general.



