

MAT 7003 : Mathematical Foundations

(for Software Engineering)

J Paul Gibson, A207

`paul.gibson@it-sudparis.eu`

<http://www-public.it-sudparis.eu/~gibson/Teaching/MAT7003/>

Algebraic Structures

<http://www-public.it-sudparis.eu/~gibson/Teaching/MAT7003/L5-AlgebraicStructures.pdf>

Algebraic Structures

DEFINITION: An *algebraic structure* consists of one or more sets closed under one or more operations, satisfying some axioms

If the axioms defining a structure are all identities, the structure is sometimes known as a *variety*

Simple Structures have no binary operations:

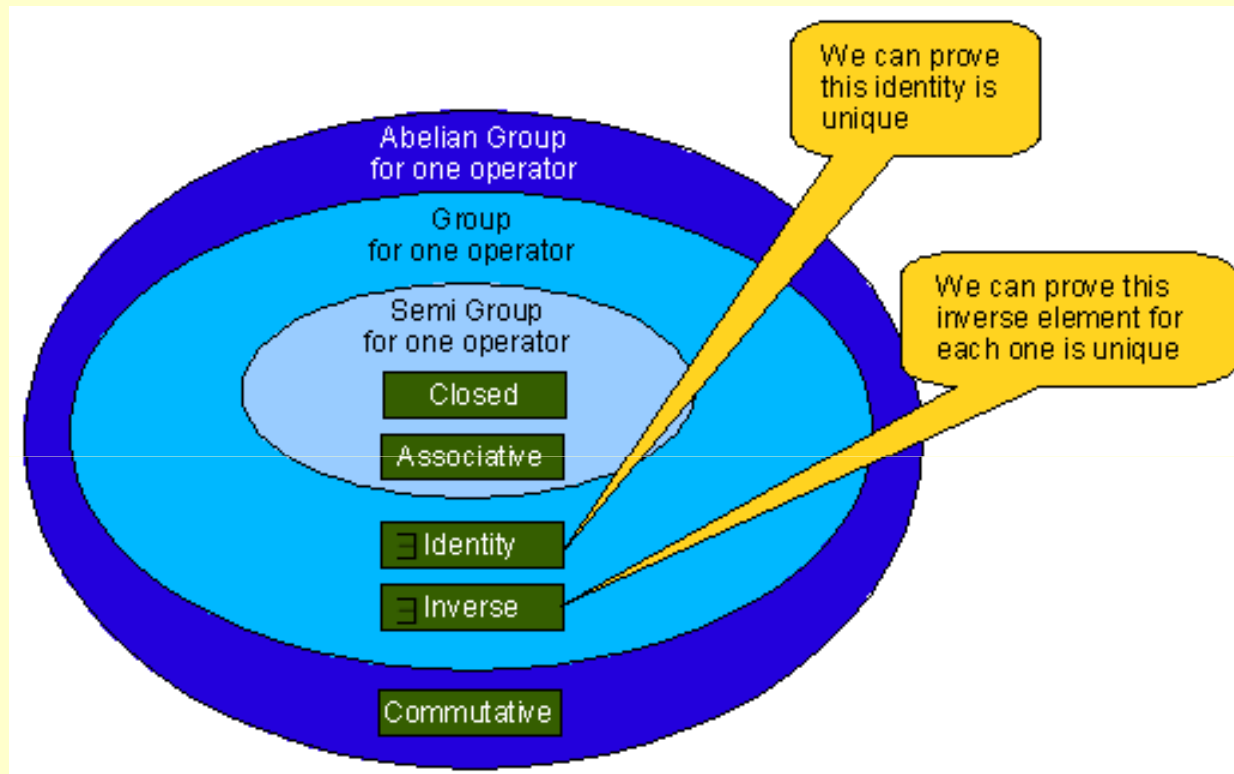
- A unary system has a single set S , a single unary operation
- The set may/may not be pointed: ie have one or more « special elements »

Algebraic Structures: from wikipedia

Algebraic structures	
Magma	Set S with binary operation $+$
Semigroup	Associativity of $+$
Monoid	Existence of identity element for $+$ in S
Group	Existence of inverse elements for $+$ in S
Abelian group	Commutativity of $+$
Pseudo-ring	Associative binary operation \cdot Distributivity of \cdot over $+$
Ring	Existence of identity element for \cdot in S
Commutative ring	Commutativity of \cdot
Field	Existence of inverse elements for \cdot in S

Group-like structures				
	Totality	Associativity	Identity	Inverses
Group	Yes	Yes	Yes	Yes
Monoid	Yes	Yes	Yes	No
Semigroup	Yes	Yes	No	No
Loop	Yes	No	Yes	Yes
Quasigroup	Yes	No	No	Yes
Magma	Yes	No	No	No

Algebraic Structures: groups



Algebraic Structures: groups

A group is a set G with just **one binary operation**, satisfying four axioms:

(G0) (*Closure law*) For any $g, h \in G$, we have $g \circ h \in G$.

(G1) (*Associative law*) For any $g, h, k \in G$, we have $(g \circ h) \circ k = g \circ (h \circ k)$.

(G2) (*Identity law*) There is an element $e \in G$ with the property that $g \circ e = e \circ g = g$ for all $g \in G$. (The element e is called the *identity element* of G .)

(G3) (*Inverse law*) For any element $g \in G$, there is an element $h \in G$ satisfying $g \circ h = h \circ g = e$. (We denote this element h by g^{-1} , and call it the *inverse* of g .)

If a group G also satisfies the commutative law, it is called a Commutative Group or an Abelian Group

(G4) (*Commutative law*) For any $g, h \in G$, we have $g \circ h = h \circ g$,

Algebraic Structures: groups

If we are only interested in Abelian groups, we use:

- $+$ as the symbol for the group operation,
- 0 for the group identity, and
- $-g$ for the inverse of g

The *order of a group* is the number of elements of the group. It may be finite (in which case it is a positive integer), or infinite.

Algebraic Structures: permutations

Let X be any set. A permutation of X is a function $g : X \rightarrow X$ which is 1-1 and onto, that is, a bijection from X to X .

Now we define an operation on permutations as follows. If g is a permutation, denote the image of the element $x \in \{1, \dots, n\}$ by xg . (As with homomorphisms, we write the function on the right of its input.) Now if g and h are two permutations, their composition g_1g_2 is defined by

$$x(gh) = (xg)h \text{ for all } x \in \{1, \dots, n\}.$$

In other words the rule is “apply g , then h ”.

For example, if g is the permutation $(1,3,5)(2,4)(6)$ in our above example, and $h = (1,2,3,4,5,6)$, then $gh = (1,4,3,6)(2,5)$. You are strongly urged to practice composing permutations given in cycle form!

The set S_n of permutations of $\{1, \dots, n\}$, with the operation of composition as defined above, is a group.

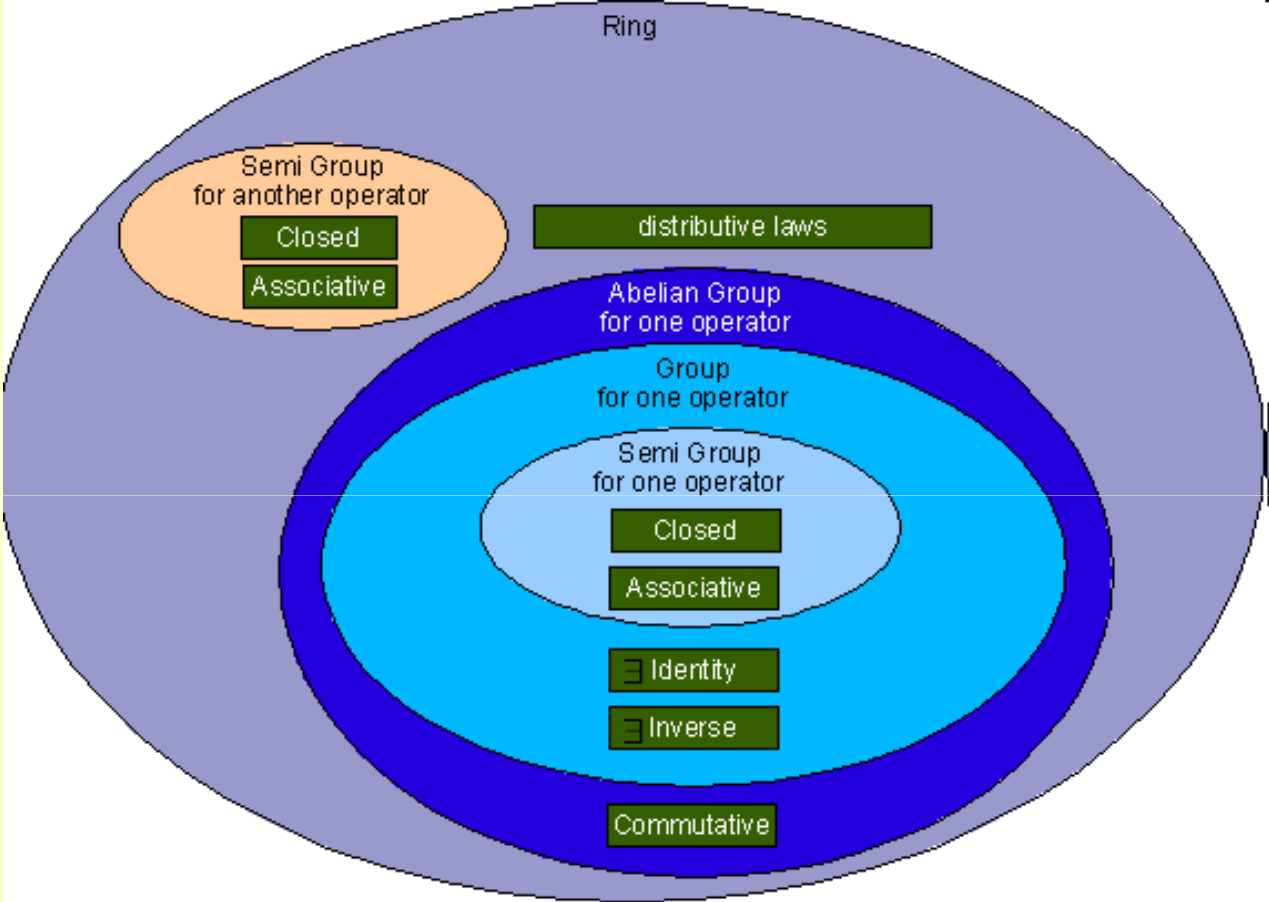
Algebraic Structures: subgroups

DEFINITION: A subgroup of a group G is a subset of G which is a subgroup in its own right (with the same group operation).

We may return to subgroups (and specialisations) in later lectures. For now, you just need to know how they are defined.

You will get a better understanding of groups when we consider rings.

Algebraic Structures: groups and rings



Algebraic Structures: rings

- A ring can be thought of as a generalisation of the integers, \mathbb{Z} .
- A ring has two operations: the first is called addition and is denoted by $+$ (with infix notation); the second is called multiplication, and is usually denoted by juxtaposition (but sometimes by \cdot with infix notation).
- We are interested in such questions as:
 - factorisation into primes,
 - construction of “modular arithmetic”,
 - etc..

Algebraic Structures: rings

We define a ring to be a set R with two binary operations satisfying the following axioms or addition and multiplication:

Axioms for addition:

- (A0) (*Closure law*) For any $a, b \in R$, we have $a + b \in R$.
- (A1) (*Associative law*) For any $a, b, c \in R$, we have $(a + b) + c = a + (b + c)$.
- (A2) (*Identity law*) There is an element $0 \in R$ with the property that $a + 0 = 0 + a = a$ for all $a \in R$. (The element 0 is called the *zero element* of R .)
- (A3) (*Inverse law*) For any element $a \in R$, there is an element $b \in R$ satisfying $a + b = b + a = 0$. (We denote this element b by $-a$, and call it the *additive inverse* or *negative* of a .)
- (A4) (*Commutative law*) For any $a, b \in R$, we have $a + b = b + a$.

It is easy to show that these elements are unique

A0 is not strictly necessary as $+$ is a binary operation

Algebraic Structures: rings

We define a ring to be a set R with two binary operations satisfying the following axioms or addition and multiplication:

Axioms for multiplication:

(M0) (*Closure law*) For any $a, b \in R$, we have $ab \in R$.

(M1) (*Associative law*) For any $a, b, c \in R$, we have $(ab)c = a(bc)$.

Mixed axiom:

(D) (*Distributive laws*) For any $a, b, c \in R$, we have $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$.

M0 is not strictly necessary as \cdot is a binary operation

Algebraic Structures: more specialised rings

A *ring with identity* follows the following *identity law*:

(*Identity law*) There is an element $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$. (The element 1 is called the *identity element* of R .)

A *division ring* is a ring with identity which also follows the *inverse law*:

(*Inverse law*) For any $a \in R$, if $a \neq 0$, then there exists an element $b \in R$ such that $ab = ba = 1$. (We denote this element b by a^{-1} , and call it the *multiplicative inverse* of a .)

A *commutative ring* is a ring where multiplication is commutative:

(*Commutative law*) For all $a, b \in R$, we have $ab = ba$.

A ring which satisfies all three further properties (that is, a *commutative division ring*) is called a *field*.

Algebraic Structures: familiar examples

The most important example of a ring is the set \mathbb{Z} of integers, with the usual addition and multiplication.

- The various properties should be familiar to you; we will simply accept that they hold.
- \mathbb{Z} is a commutative ring with identity. It is not a division ring because, e.g. there is no integer b satisfying $2b = 1$.
- Note that the set \mathbb{N} of natural numbers, or non-negative integers, is not a ring, since it fails the inverse law for addition. (There is no non-negative integer b such that $2+b = 0$.)

The rational numbers \mathbb{Q} , the real numbers \mathbb{R} , and the complex numbers \mathbb{C} , are fields

Algebraic Structures: matrices/tables

Let R be a ring. Then the set $M_n(R)$ of $n \times n$ matrices over R , with addition and multiplication defined in the usual way, is a ring.

If R has an identity, then $M_n(R)$ has an identity; but it is not in general a commutative ring or a division ring.

Algebraic Structures: power sets

Let $P(A)$, the power set of A , be the set of all subsets of the set A .

Now we define addition and multiplication on $P(A)$ to be the operations of symmetric difference and intersection respectively:

$$x + y = x \Delta y, \quad xy = x \cap y.$$

The set $P(A)$, with the above operations, is a ring; it is commutative, has an identity element, but is not a field if $|A| > 1$. It satisfies the further conditions $x+x = 0$ and $xx = x$ for all x .

Algebraic Structures: modular arithmetic

For any positive integer n , Z_n is a commutative ring with identity.

It is a field if and only if n is a prime number.

For example, in Z_5 $2^{-1} = 3$

$+$	0	1	2	3	4	\cdot	0	1	2	3	4
0	0	1	2	3	4	0	0	0	0	0	0
1	1	2	3	4	0	1	0	1	2	3	4
2	2	3	4	0	1	2	0	2	4	1	3
3	3	4	0	1	2	3	0	3	1	4	2
4	4	0	1	2	3	4	0	4	3	2	1

Algebraic Structures: *Isomorphism*

Here are the addition and multiplication tables of a ring with two elements, which for now I will call o and i .

$$\begin{array}{c|cc} + & o & i \\ \hline o & o & i \\ i & i & o \end{array} \qquad \begin{array}{c|cc} \cdot & o & i \\ \hline o & o & o \\ i & o & i \end{array}$$

You may recognise this ring in various guises: it is the Boolean ring $\mathcal{P}(X)$, where $X = \{x\}$ is a set with just one element x ; we have $o = \emptyset$ and $i = \{x\}$. Alternatively it is the ring of integers mod 2, with $o = [0]_2$ and $i = [1]_2$.

The fact that these two rings have the same addition and multiplication tables shows that, from an algebraic point of view, we cannot distinguish between them.

Algebraic Structures: *Isomorphism*

We formalise this as follows. Let R_1 and R_2 be rings. Let $\theta : R_1 \rightarrow R_2$ be a function which is one-to-one and onto, that is, a bijection between R_1 and R_2 . Now we denote the result of applying the function θ to an element $r \in R_1$ by $r\theta$ or $(r)\theta$ rather than by $\theta(r)$; that is, we write the function on the right of its argument.

Now we say that θ is an *isomorphism* from R_1 to R_2 if it is a bijection which satisfies

$$(r_1 + r_2)\theta = r_1\theta + r_2\theta, \quad (r_1r_2)\theta = (r_1\theta)(r_2\theta).$$

This means that we “match up” elements in R_1 with elements in R_2 so that addition and multiplication work in the same way in both rings.

Algebraic Structures: *Isomorphism*

Example To return to our earlier example, let $R_1 = \mathcal{P}(\{x\})$ and let R_2 be the ring of integers mod 2, and define a function $\theta : R_1 \rightarrow R_2$ by

$$0\theta = [0]_2, \quad \{x\}\theta = [1]_2.$$

Then θ is an isomorphism.

- We say that the rings R_1 and R_2 are “isomorphic” if there is an isomorphism from R_1 to R_2 .
- The word “isomorphic” means, roughly speaking, “the same shape”: if two rings are isomorphic then they can be regarded as identical from the point of view of Ring Theory

We use the notation $R_1 \cong R_2$ to mean “ R_1 is isomorphic to R_2 ”.

Algebraic Structures: *Homomorphism*

An isomorphism is a function between rings with two properties: it is a bijection (one-to-one and onto), and it preserves addition and multiplication (as expressed by equation (2.1)). A function which preserves addition and multiplication but is not necessarily a bijection is called a homomorphism. Thus, a *homomorphism* from R_1 to R_2 is a function $\theta : R_1 \rightarrow R_2$ satisfying

$$(r_1 + r_2)\theta = r_1\theta + r_2\theta, \quad (r_1r_2)\theta = (r_1\theta)(r_2\theta).$$

For example, the function from the ring \mathbb{Z} to the ring of integers mod 2, which takes the integer n to its congruence class $[n]_2 \pmod{2}$, is a homomorphism. Basically this says that, if we only care about the parity of an integer, its congruence mod 2, then the addition and multiplication tables are

$+$	even	odd	\cdot	even	odd
even	even	odd	even	even	even
odd	odd	even	odd	even	odd

and this ring is the same as the one at the start of this section.

Algebraic Structures: *Unique Factorisation in rings*

One of the most important properties of the integers is that any number can be factorised into prime factors in a unique way.

But we have to be a bit careful: It would be silly to try to factorise 0 or 1; and the factorisation is not quite unique, since $(-2) \cdot (-3) = 2 \cdot 3$, for example.

Once we have the definitions straight, we can see that “unique factorisation” holds in a large class of rings.

We return to this when we look at number theory (in a later lecture)

Algebraic Structures: *Unique Factorisation in rings*

TO DO:

Write a program that can find the *unique prime factors* of any given integer.

Test the code against an Event-B specification