Axioms and algebraic systems*

Leong Yu Kiang
Department of Mathematics
National University of Singapore

In this talk, we introduce the important concept of a group, mention some equivalent sets of axioms for groups, and point out the relationship between the individual axioms. We also mention briefly the definitions of a ring and a field.

Definition 1. A *binary operation* on a non-empty set S is a rule which associates to each ordered pair (a, b) of elements of S a unique element, denoted by $a * b$, in S. The binary relation itself is often denoted by $*$. It may also be considered as a mapping from $S \times S$ to S, i.e., $* : S \times S \to S$, where $(a, b) \to a * b$, $a, b \in S$.

Example 1. Ordinary addition and multiplication of real numbers are binary operations on the set $\mathbb{R}$ of real numbers. We write $a + b$, $a \cdot b$ respectively. Ordinary division $\div$ is a binary relation on the set $\mathbb{R}^*$ of non-zero real numbers. We write $a \div b$.

Definition 2. A binary relation $*$ on S is *associative* if for every a, b, c in S,

$$(a * b) * c = a * (b * c).$$

Example 2. The binary operations $+$ and $\cdot$ on $\mathbb{R}$ (Example 1) are associative. The binary relation $\div$ on $\mathbb{R}^*$ (Example 1) is not associative since

$$(1 \div 2) \div 3 = \frac{1}{6} \neq \frac{3}{2} = 1 \div (2 \div 3).$$

---

* Talk given at the Workshop on Algebraic Structures organized by the Singapore Mathematical Society for school teachers on 5 September 1988.

Definition 3. A *semi-group* is a non-empty set S together with an associative binary operation $*$, and is denoted by $(S, *)$.

Example 3. The set of $n \times n$ matrices with entries from $\mathbb{R}$ together with matrix multiplication $\cdot$ is a semi-group. This is denoted by $(M_n(\mathbb{R}), \cdot)$. In particular

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Definition 4. An element e of a semi-group is an *identity* element of S if for all $a \in S$,

$$e * a = a = a * e.$$

Example 4. Let $(\mathbb{R}, +)$ be the semi-group under ordinary addition $+$. Then 0 is an identity of $\mathbb{R} : 0 + a = a = a + 0$ for every $a \in \mathbb{R}$.

Example 5. Let $(\mathbb{R}, \cdot)$ be the semi-group under ordinary multiplication. Then 1 is the identity: $1 \cdot a = a = a \cdot 1$ for every $a \in \mathbb{R}$.

Definition 5. A *monoid* is a semi-group with an identity element.

Example 6. $(M_n(\mathbb{R}), \cdot)$ is a monoid under matrix multiplication with the $n \times n$ identity matrix as an identity element.

Definition 6. An element x of a monoid S is *invertible* if there is an element x' in S such that $x' * x = e = x * x'$, where e is an identity element in S. Such an element x' is called an *inverse* of x.

Example 7. In the monoid $(M_n(\mathbb{R}), \cdot)$, x is invertible if and only if $\det x \neq 0$.

Remarks. If a monoid S has an identity element, then it is unique. That is, if e, $e' \in S$ such that for all $a \in S$,

$$e * a = a = a * e, \qquad e' * a = a = a * e',$$

then $e = e'$. For we have $e = e * e' = e'$.

If an element x of a monoid S is invertible, then x has a unique inverse. That is, if x_1, $x_2 \in S$ and

$$x_1 * x = e = x * x_1, \qquad x_2 * x = e = x * x_2,$$

then $x_1 = x_2$. For we have

$$x_1 = x_1 * e = x_1 * (x * x_2) = (x_1 * x) * x_2 = e * x_2 = x_2.$$

Thus we will simply say *the* identity (element) of S and *the* inverse of x.

Definition 7. A *group* is a monoid G in which every element is invertible.

Example 8. The set of $n \times n$ matrices with entries from $\mathbb{R}$ and non-zero determinant is a group under matrix multiplication. This group is denoted by $GL_n(\mathbb{R})$ and called the ***general linear group of degree n over*** $\mathbb{R}$.

Axioms of a group. A group is a non-empty set G with a binary operation $*$ satisfying the following properties.

Axiom 1. (Associativity) The binary operation $*$ is associative.

Axiom 2. (Identity) G has an identity element.

Axiom 3. (Inverse) Every element of G is invertible.

Independence of the group axioms. The above three axioms (1), (2), (3) are independent of each other.

Example 9. $(M_n(\mathbb{R}), \cdot)$ in Example 3 is an example of an algebraic system satisfying Axioms (1), (2) but not (3).

Example 10. Let $S = \{a, b, c\}$ be a set of 3 elements with a binary operation $*$ given by the multiplication table

*	a	b	c
a	a	b	c
b	b	a	c
c	c	b	a

For example, $b * c = c$, $c * b = b$. The element a is the identity in S and every element in S has an inverse: $a * a = b * b = c * c = a$. But $*$ is not associative:

$$b * (c * b) = b * b = a,$$

$$(b * c) * b = c * b = b.$$

Hence $(S, *)$ satisfies Axioms (2), (3) but not (1).

Alternative axioms of a group. A group is a non-empty set G with a binary operation $*$ satisfying

Axiom 1. (Associativity) The binary operation $*$ is associative.

Axiom 2′. (Left identity) G has a "left identity" e_l such that $e_l * a = a$ for all a in G.

Axiom 3′. (Left inverse) Each element a in G has a "left inverse" a_l such that $a_l * a = e_l$.

The axioms 2′, 3′ may be replaced by the following Axioms 2″, 3″.

Axiom 2″. (Right identity) G has a "right identity" e_r such that $a * e_r = a$ for all a in G.

Axiom 3″. (Right inverse) Each element a in G has a "right inverse" a_r such that $a * a_r = e_r$.

Theorem 1. *Axioms 1, 2, 3 are equivalent to Axioms 1, 2′, 3′, and to Axioms 1, 2″, 3″.*

Proof. Clearly, Axioms 1, 2, 3 imply Axioms 1, 2′, 3′. Conversely, assume Axioms 1, 2′, 3′. Let a be any element of G. From Axiom 3′, we have

$$(a_l * a) * a_l = e_l * a_l = a_l \tag{1}$$

Let b be a left inverse of a_l, i.e., $b * a_l = e_l$. Multiplying (1) by b on the left hand side, and using Axiom 1, we have

$$(b * a_l) * (a * a_l) = b * a_l,$$

or

$$e_l * (a * a_l) = e_l,$$

by choice of b. Hence by Axiom 2′,

$$a * a_l = e_l. \tag{2}$$

Finally, we have

$$a * (a_l * a) = a * e_l,$$

or

$$(a * a_l) * a = a * e_l,$$

or, by (2),

$$e_l * a = a * e_l. \tag{3}$$

(2) and (3) show that e_l is the identity of G and a_l is the inverse of a.

We can similarly show that Axioms 1, 2, 3 are equivalent to Axioms $1, 2'', 3''$. □

Example 11. There is an algebraic system which is not a group but which satisfies Axioms 1, 2′ and Axiom 3″: For each element $a \in G$, there is an element $a' \in G$ such that $a * a' = e_l$, where e_l is a left identity of G.

Let $S = \{a, b\}$ be a set of two elements with binary operation $*$ given by

$$a * a = a, \qquad a * b = b,$$
$$b * a = a, \qquad b * b = b.$$

It can be easily checked that $*$ is associative. The element a is a left identity of S. Moreover, the element a is a "right inverse" of both a and b with respect to the left identity a, i.e., $a * a = a$, $b * a = a$. However, S has no right identity and hence $(S, *)$ cannot be a group.

Example 12. $(\mathbb{R}^*, \div)$ in Example 1 satisfies Axioms 2′, 3′ but not Axiom 1. In fact, 1 is a right identity and every element a in $\mathbb{R}^*$ is its own inverse: $a \div 1 = a$, $a \div a = 1$.

Theorem 2. *Let G be a semi-group with binary operation $*$. Suppose for any a, b in G, the equations $a * x = b$ and $y * a = b$ have solutions with x, y in G. Then $(G, *)$ is a group.*

Proof. Let a be any fixed element in G. Then the equation $a * x = a$ has a solution $x = x_0$ say : $a * x_0 = a$. We will show that $b * x_0 = b$ for *every* b in G. Let b be any element in G. Then the equation $y * a = b$ has a solution $y = y_0$ say. Hence

$$b * x_0 = (y_0 * a) * x_0 = y_0 * (a * x_0) = y_0 * a = b.$$

In other words, x_0 is a right identity of G.

Also, for any b in G, the equation $b * x = x_0$ has a solution $x = b'$ say. That is, b has a "right inverse". Hence $(G, *)$ satisfies Axioms 1, 2″, 3″and is a group by Theorem 1. □

Example 13. Let S be a set consisting of at least 2 elements and define a binary operation $*$ on S as follows :

$$a * b = b \quad \text{for all} \quad a, b \in S.$$

Then the equation $a * x = b$ has a solution in x, namely $x = b$, and $(S, *)$ is a semi-group but not a group.

Proof. Associativity of $*$ follows from

$$(a * b) * c = b * c = c,$$

$$a * (b * c) = a * c = c.$$

Hence S is a semi-group. Suppose S is a group. Let e be the identity and let a be an element of S with $a \neq e$. (This is possible since S has at least 2 elements.) Then $a * e = a$, by Axiom 2, and $a * e = e$, by definition of $*$. Hence $a = e$: a contradiction. So $(S, *)$ cannot be a group. □

Note. In Example 13, it follows from the definition of $*$ that the equation $y * a = b$ has no solution with y in S if $a \neq b$.

Theorem 3. *Let G be a finite semi-group with binary operation $*$. Suppose G satisfies the following cancellation laws.*
(Left cancellation law). If a, x, y are in G such that $a * x = a * y$, then

$$x = y.$$

(Right cancellation law). If a, x, y are in G such that $x * a = y * a$, then

$$x = y.$$

Then $(G, *)$ is a group.

Proof. We will show that for any given a, b in G, the equations $a * x = b$ and $y * a = b$ have solutions in G. Suppose G has exactly n elements :

$$G = \{a_1, \ldots, a_n\}.$$

For a given a_i in G, consider the following subset of G :

$$X = \{a_i * a_1, \ldots, a_i * a_n\}.$$

Now X has exactly n elements since $a_i * a_j = a_i * a_k$ implies that $a_j = a_k$ by the left cancellation law. Hence $X = G$. Thus for any a_j in G, there is some a_r in G such that $a_i * a_r = a_j$.

Similarly, the right cancellation law implies that

$$G = \{a_1 * a_i, \ldots, a_n * a_i\}$$

and hence $y * a_i = a_j$ has a solution with y in G. Hence, by Theorem 2, $(G, *)$ is a group. □

Example 14. Let S be the semi-group given in Example 13. Then S satisfies the left cancellation law. For if $a * x = a * y$, then by definition of $*$, we have $x = y$. However, S does not satisfy the right cancellation law for the equation $x * a = y * a$ holds for all $x, y \in G$. From Example 13, $(S, *)$ is not a group.

Example 15. If the condition of G being finite is removed from Theorem 3, then G need not be a group. Take G to be the set of positive integers

$$G = \{1, 2, 3, \ldots, n, \ldots\},$$

and let $*$ be ordinary multiplication of integers. Then G is an infinite semi-group satisfying the left and right cancellation laws but G is not a group since every integer greater than 1 has no multiplicative inverse.

Notation. If G is a group with binary operation $*$, we often write

$$a \cdot b = a * b, \quad \text{or simply,} \quad ab = a * b.$$

We also write $a^1 = a$, and for $n > 2$, $a^n = a^{n-1} \cdot a$. The inverse of a is denoted by a^{-1}, and for $n < -1$, write $m = -n$, and $a^n = (a^{-1})^m$. The usual rules hold : For all integers m, n,

$$a^{m+n} = a^m \cdot a^n, \quad (a^m)^n = a^{mn}.$$

Definition 8. The *order* of an element a of a group G is the smallest positive integer n for which $a^n = e$, where e is the identity of G. If no such integer exists, the element a is said to be of *infinite* order. The order of a is denoted by $\mathrm{o}(a)$.

Example 16. The product of two elements of finite order can be of infinite order. For if

$$a = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix},$$

then

$$ab = \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix}.$$

Thus $\mathrm{o}(a) = 2$, $\mathrm{o}(b) = 2$, but ab is of infinite order.

Theorem 4. *Let a be an element of a group G. If $a^k = e$, where e is the identity of G, then $\mathrm{o}(a)$ divides k.*

Proof. Let $n = o(a)$, and write $k = nq + r$, where q, r are integers with $0 \le r < n$. Then

$$e = a^k = (a^n)^q . a^r = a^r.$$

Since $0 \le r < n$ and n is the smallest positive integer for which $a^n = e$, it follows that $k = nq$. □

Example 17. Let p be a prime, and for $n \ge 1$, define $\mathbb{C}_{p^n}$ to be the multiplicative group of complex p^n-th roots of unity :

$$\mathbb{C}_{p^n} = \{z \in \mathbb{C} : z^{p^n} = 1\}.$$

Let $G = \bigcup_{n=1}^{\infty} \mathbb{C}_{p^n}$. Then G is an infinite group in which every element is of finite order.

The above group G is called a *quasi-cyclic* group.

Definition 9. A group G is *abelian* if $ab = ba$ for all a, b in G.

Example 18. The following groups are abelian.

(a) The group $\mathbb{Z}$ of integers under ordinary addition,
(b) The group $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ under addition modulo n,
(c) The group $\mathbb{R}$ of real numbers under ordinary addition,
(d) The group $\mathbb{C}$ of complex numbers under ordinary addition,
(e) The group of rotations in the xy-plane about the origin under composition of rotations.

If $n > 1$, the group $GL_n(\mathbb{R})$ (see Example 8) is non-abelian.

Axioms of a ring. Let R be a non-empty set with two binary operations $+$ and $\cdot$ (called *addition* and *multiplication*). R is a *ring* if it satisfies the following axioms.

Axiom 1. R is an additive abelian group with respect to $+$.

Axiom 2. R is a multiplicative semi-group with respect to $\cdot$.

Axiom 3. (Distributive laws). For all a, b, c in R,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

We denote the ring by $(R, +, \cdot)$. The identity of the additive group of R is called the *zero* element of R and is denoted by 0.

Example 19. The following are rings with the usual binary operations.

(a) $\mathbb{Z}$: the ring of integers,

(b) $\mathbb{Q}$: the ring of rational numbers,

(c) $\mathbb{R}$: the ring of real numbers,

(d) $\mathbb{C}$: the ring of complex numbers,

(e) $R[x]$: the ring of polynomials in the variable x with coefficients from a ring R,

(f) $M_n(R)$: the ring of $n \times n$ matrices with entries from a ring R.

In (f), two non-zero elements of $M_n(R)$ may have a product equal to 0.

Axioms of a field. Let R be a non-empty set with two binary operations $+$ and $\cdot$ (called *addition* and *multiplication*). R is a *field* if it satisfies the following axioms.

Axiom 1. R is an additive abelian group with respect to $+$.

Axiom 2. $R - \{0\}$, where 0 is the identity element with respect to $+$, is a multiplicative abelian group with respect to $\cdot$.

Axiom 3. (Distributive laws). For all a, b, c in R,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

A field is a ring $(R, +, \cdot)$ in which $(R - \{0\}, \cdot)$ is an abelian group.

Example 20. The following are fields with the usual binary operations.

(a) $\mathbb{Q}$: the field of rational numbers,

(b) $\mathbb{R}$: the field of real numbers,

(c) $\mathbb{C}$: the field of complex numbers,

Example 21. Let p be a prime, and let

$$\mathbb{Z}_p = \{0, 1, \ldots, p - 1\}.$$

Define $\oplus$ and $\otimes$ in $\mathbb{Z}_p$ as follows :

$x \oplus y =$ remainder of the ordinary sum $x + y$ when divided by p,

$x \otimes y =$ remainder of the ordinary product xy when divided by p.

Then $\mathbb{Z}_p$ is a field of p elements.

Note. A finite field must contain exactly p^n elements where p is a prime and n is a positive integer. Finite fields are called *Galois fields*, named after Evariste Galois (1811-1832) who first introduced them in his ground-breaking work on solubility of equations.

Finite fields have some recent applications to coding theory and cryptography. With the availability of fast-speed computations, these applications are of more than theoretical interest.