CHAPTER 1

# Groups

© W W L Chen, 1991, 1993, 2013.
This chapter is available free to all individuals,
on the understanding that it is not to be used for financial gain,
and may be downloaded and/or photocopied,
with or without permission from the author.
However, this document may not be kept on any information storage and retrieval system
without permission from the author,
unless such system is not accessible to any individuals other than its owners.

Consider the set $\mathbb{Z}$ of integers and the operation addition. We take the following for granted:

(i) For every $x, y \in \mathbb{Z}$, $x + y \in \mathbb{Z}$.
(ii) For every $x, y, z \in \mathbb{Z}$, $(x + y) + z = x + (y + z)$.
(iii) For every $x \in \mathbb{Z}$, $x + 0 = 0 + x = x$.
(iv) For every $x \in \mathbb{Z}$, $x + (-x) = (-x) + x = 0$.

Consider now the set $\mathbb{R} \setminus \{0\}$ of non-zero real numbers and the operation multiplication. Again we take the following for granted:

(i) For every $x, y \in \mathbb{R} \setminus \{0\}$, $xy \in \mathbb{R} \setminus \{0\}$.
(ii) For every $x, y, z \in \mathbb{R} \setminus \{0\}$, $(xy)z = x(yz)$.
(iii) For every $x \in \mathbb{R} \setminus \{0\}$, $x1 = 1x = x$.
(iv) For every $x \in \mathbb{R} \setminus \{0\}$, $xx^{-1} = x^{-1}x = 1$.

There are many more examples of sets and operations where properties analogous to $(i)$–$(iv)$ above hold. The sets do not even have to be very large. Consider the set $\{0\}$ together with the operation addition, or the set $\{\pm 1\}$ together with the operation multiplication.

This apparent similarity leads us to consider an abstract object which will incorporate all these individual cases as examples. We say that these examples all have a group structure.

## 1.1. Formal Definition

DEFINITION. A set $G$, together with a binary operation $*$, is said to form a group, denoted by $(G, *)$, if the following properties are satisfied:

(G1) (Closure) For every $x, y \in G$, $x * y \in G$.
(G2) (Associativity) For every $x, y, z \in G$, $(x * y) * z = x * (y * z)$.
(G3) (Identity) There exists $e \in G$ such that $x * e = e * x = x$ for every $x \in G$.
(G4) (Inverse) For every $x \in G$, there exists an element $x' \in G$ such that $x * x' = x' * x = e$.

REMARK. Sometimes we omit reference to the operation $*$ and simply refer to a group $G$.

EXAMPLES. (1) $(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\{0\}, +)$ and $(\{\pm 1\}, \cdot)$ are all groups.
(2) The set $\mathbb{R}$, together with multiplication, does not form a group. The element 0 has no inverse.
(3) Consider the set $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ of integers modulo 5. This has the group table for addition modulo 5 below:

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

(4) For every $n \in \mathbb{N}$, the set $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ of integers modulo $n$ forms a group under addition modulo $n$.

(5) The set $\mathcal{M}_{2,2}(\mathbb{R})$ of $2 \times 2$ matrices with entries in $\mathbb{R}$, together with matrix addition, forms a group with identity $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(6) The set $\mathcal{M}^*_{2,2}(\mathbb{R})$ of invertible $2 \times 2$ matrices with entries in $\mathbb{R}$, together with matrix multiplication, forms a group with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(7) Consider the set $S_3$ of all one-to-one functions from $\{1, 2, 3\}$ to $\{1, 2, 3\}$. Then $S_3$, together with composition of functions, forms a group. To see that, note that the composition of two one-to-one functions from $\{1, 2, 3\}$ to $\{1, 2, 3\}$ is another one-to-one function from $\{1, 2, 3\}$ to $\{1, 2, 3\}$, so that (G1) is satisfied. (G2) is satisfied in view of the associativity of composition of functions. On the other hand, the function $i : \{1, 2, 3\} \to \{1, 2, 3\}$, given by $i(x) = x$ for every $x \in \{1, 2, 3\}$, satisfies the requirements of the identity, so that (G3) is satisfied. Finally, any one-to-one function from $\{1, 2, 3\}$ to $\{1, 2, 3\}$ is also onto. It follows that the inverse function exists, so that (G4) is satisfied.

Note that matrix multiplication is not commutative. In particular, if $A, B \in \mathcal{M}^*_{2,2}(\mathbb{R})$, then it is not guaranteed that $AB = BA$. On the other hand, composition of functions is also not commutative. In particular, if $f, g \in S_3$, then it is not guaranteed that $g \circ f = f \circ g$. Note now that in our definition of a group, we have not included the rule that $x * y = y * x$ for every $x, y \in G$.

Definition. We say that the group $(G, *)$ is abelian if the following extra property is satisfied:

(GA) (Commutativity) For every $x, y \in G$, $x * y = y * x$.

Examples. Note that all the groups in Examples (1) and (3)–(5) above are abelian, while the groups in Examples (6) and (7) above are not.

## 1.2. Elementary Properties

There are a few simple consequences which can be easily deduced from the definition of a group.

Proposition 1.1. *Suppose that $(G, *)$ is a group, and that $a, x, y \in G$. Then*

(i) (Left cancellation) *if $a * x = a * y$, then $x = y$; and*
(ii) (Right cancellation) *if $x * a = y * a$, then $x = y$.*

Proof. (i) If $a * x = a * y$, then $a' \in G$ by (G4) and

$$a' * (a * x) = a' * (a * y). \tag{1.1}$$

On the other hand, by (G2), (G4) and (G3),

$$a' * (a * x) = (a' * a) * x = e * x = x. \tag{1.2}$$

Similarly

$$a' * (a * y) = y. \tag{1.3}$$

The result now follows on combining (1.1)–(1.3).

(ii) can be proved in a similar way. ◯

Proposition 1.2. *Suppose that $(G, *)$ is a group. Then the identity element $e$ is unique.*

Proof. Note that if $e_1$ and $e_2$ both satisfy the requirements for being the identity element, then $e_1 = e_1 * e_2 = e_2$. ◯

Proposition 1.3. *Suppose that $(G, *)$ is a group, and that $x \in G$. Then the inverse element $x'$ is unique. On the other hand, for every $x, y \in G$, we have $(x * y)' = y' * x'$.*

Proof. Note that if $x_1$ and $x_2$ both satisfy the requirements for being the inverse element of $x$, then $x * x_1 = e = x * x_2$, so that $x_1 = x_2$ in view of left cancellation. On the other hand,

$$(y' * x') * (x * y) = \ldots = e \quad \text{and} \quad (x * y) * (y' * x') = \ldots = e,$$

so that $y' * x'$ satisfies the requirements for being the inverse of $x * y$. It follows that $(x * y)' = y' * x'$ by the uniqueness of inverse. ◯

## 1.3. Subgroups

Recall that $(\mathbb{Z},+)$ forms a group, and so does $(\{0\},+)$. Another example is that $(\mathbb{R}\setminus\{0\},\cdot)$ forms a group, and so does $(\{\pm1\},\cdot)$. Clearly $\{0\}\subset\mathbb{Z}$ and $\{\pm1\}\subset\mathbb{R}\setminus\{0\}$. We can therefore say that $(\{0\},+)$ "is smaller than" $(\mathbb{Z},+)$, and that $(\{\pm1\},\cdot)$ "is smaller than" $(\mathbb{R}\setminus\{0\},\cdot)$.

DEFINITION. Suppose that $(G,*)$ is a group, and that $H\subseteq G$. Then we say that $H$ is a subgroup of $G$ if $H$, under the same binary operation $*$, forms a group.

EXAMPLES. (1) $(\{0\},+)$ is a subgroup of $(\mathbb{Z},+)$.
(2) $(\{\pm1\},\cdot)$ is a subgroup of $(\mathbb{R}\setminus\{0\},\cdot)$.
(3) Consider the group $(\mathbb{Z}_8,+)$, where $+$ denotes addition modulo 8. If $H=\{0,2,4,6\}$, then $(H,+)$, where $+$ again denotes addition modulo 8, is a subgroup of $(\mathbb{Z}_8,+)$.
(4) $(\mathbb{Z}_8,+)$ forms a group. $(\mathbb{Z}_4,+)$ also forms a group. On the other hand,

$$\mathbb{Z}_4=\{0,1,2,3\}\subset\{0,1,2,3,4,5,6,7\}=\mathbb{Z}_8.$$

So $(\mathbb{Z}_4,+)$ is a subgroup of $(\mathbb{Z}_8,+)$. What is wrong with this argument? Find two mistakes.
(5) Any group is a subgroup of itself. On the other hand, the set $\{e\}$, together with the group operation, forms a subgroup. These are usually called the trivial subgroups.

DEFINITION. Suppose that $(G,*)$ is a group, and that $H$ is a subgroup of $G$. Suppose further that $H\neq\{e\}$ and $H\neq G$. Then we say that $H$ is a proper subgroup of $G$.

THEOREM 1.4. *Suppose that the group $(G,*)$ has identity element $e$, and that $H\subseteq G$. Then $H$ is a subgroup of $G$ if the following conditions are satisfied:*

(S1) $e\in H$.
(S2) *For every $x,y\in H$, $x*y\in H$.*
(S3) *For every $x\in H$, $x'\in H$.*

PROOF. (G1) for $H$ follows from (S2). (G2) for $H$ is weaker than (G2) for $G$. (G3) for $H$ follows from (G3) for $G$ and (S1). Finally (G4) for $H$ follows from (G4) for $G$ and (S3). ◯

THEOREM 1.5. *Suppose that $(G,*)$ is a group, and that $H$ is a non-empty subset of $G$. Then $H$ is a subgroup of $G$ if the following condition is satisfied:*

(SG) *For every $x,y\in H$, $x*y'\in H$.*

PROOF. Take any $x\in H$. Then by (SG), $e=x*x'\in H$, so that (S1) follows. For every $x\in H$, it follows from (S1) and (SG) that $x'=e*x'\in H$, so that (S3) follows. Finally, for every $x,y\in H$, it follows from (S3) that $y'\in H$; in view of (SG), $x*y=x*(y')'\in H$, so that (S2) follows. The result now follows from Theorem 1.4. ◯

EXAMPLES. (1) Let $H=\{3n:n\in\mathbb{Z}\}$. Then $(H,+)$ is a subgroup of $(\mathbb{Z},+)$.
(2) Let $H=\{2^n:n\in\mathbb{Z}\}$. Then $(H,\cdot)$ is a subgroup of $(\mathbb{R}\setminus\{0\},\cdot)$.

In many instances, it is convenient to use multiplicative notation to describe the binary operation $*$, *i.e.* we write $xy$ instead of $x*y$. If $x$ is an element of a group $G$, we can then define $x^0=e$ and $x^1=x$; for every $n\in\mathbb{N}$, we define $x^{n+1}=x^nx$ and $x^{-n}=(x')^n$. Then it is not difficult to prove that for every $m,n\in\mathbb{Z}$, we have $x^mx^n=x^{m+n}$ and $(x^m)^n=x^{mn}$.

REMARK. Suppose that $x$ and $y$ are elements of a group. It is not always true that $(xy)^n=x^ny^n$. Try to find a counterexample in the multiplicative group $\mathcal{M}^*_{2,2}(\mathbb{R})$. On the other hand, try to convince yourself that equality always holds for abelian groups.

## 1.4. Special Subgroups

Our first type of subgroups are obtained by building from a particular element of the group.

THEOREM 1.6. *Suppose that $(G,*)$ is a group, and that $a\in G$. Suppose further that*

$$\langle a\rangle=\{a^n:n\in\mathbb{Z}\}.$$

*Then $\langle a\rangle$ is a subgroup of $G$.*

PROOF. Clearly $\langle a \rangle$ is non-empty. Suppose that $x, y \in \langle a \rangle$. Then there exist $m, n \in \mathbb{Z}$ such that $x = a^m$ and $y = a^n$. Then $x * y' = a^m a^{-n} = a^{m-n} \in \langle a \rangle$, since $m - n \in \mathbb{Z}$. The result now follows from Theorem 1.5. ◯

DEFINITION. We say that the group $\langle a \rangle$ in Theorem 1.6 is the cyclic subgroup of $G$ generated by the element $a$.

PROPOSITION 1.7. *Suppose that $(G, *)$ is a group, and that $a \in G$. Suppose further that $H$ is a subgroup of $G$, and that $a \in H$. Then $\langle a \rangle \subseteq H$. In other words, $\langle a \rangle$ is the smallest subgroup of $G$ containing $a$.*

PROOF. Clearly $a^0 \in H$, since $a^0 = e$ and $H$ is a group. Suppose that $n \in \mathbb{N}$ and $n \geqslant 2$. Then since $H$ is a group and $a^2 = aa, \ldots, a^n = a^{n-1}a$, it can be shown by induction that $a^n \in H$ for every $n \in \mathbb{N}$. Suppose now that $-n \in \mathbb{N}$. Then $a^{-n} \in H$, and since $a^n$ is the inverse of $a^{-n}$, we must have $a^n \in H$. It follows that $a^n \in H$ for every $n \in \mathbb{Z}$. ◯

EXAMPLE. Consider the subgroup $\langle 4 \rangle$ of $(\mathbb{Z}, +)$. Note carefully that we have $4^2 = 4 + 4$ and $4^{-3} = (-4) + (-4) + (-4)$. It is not difficult to see that $\langle 4 \rangle = \{4n : n \in \mathbb{Z}\}$.

THEOREM 1.8. *Suppose that $(G, *)$ is a group with identity element $e$, and that $a \in G$. Then precisely one of the following is true:*

(i) *For every $n \in \mathbb{N}$, $a^n \neq e$. Also, for every $m, n \in \mathbb{Z}$, $a^m \neq a^n$. The set $\langle a \rangle$ is infinite.*
(ii) *There exists a smallest $m \in \mathbb{N}$ such that $\langle a \rangle = \{a, a^2, \ldots, a^m\}$.*

PROOF. Either (i) for every $n \in \mathbb{N}$, $a^n \neq e$; or (ii) there exists $n \in \mathbb{N}$ such that $a^n = e$; but not both.

(i) Suppose on the contrary that there exist $m, n \in \mathbb{Z}$ such that $m \neq n$ and $a^m = a^n$. Without loss of generality, assume that $m > n$. Then clearly $a^{m-n} = a^m a^{-n} = a^m (a^n)' = a^m (a^m)' = e$, a contradiction.

(ii) Consider the set $S = \{n \in \mathbb{N} : a^n = e\}$. Since $S$ is a non-empty set of natural numbers, it has a smallest element, $m$ say. Then $a^m = e$. Now every $n \in \mathbb{Z}$ can be written in the form $n = mq + r$, where $q, r \in \mathbb{Z}$ and $0 \leqslant r < m$. Then $a^n = a^{mq} a^r = (a^m)^q a^r = e^q a^r = a^r$, so clearly $\langle a \rangle \subseteq \{e, a, a^2, \ldots, a^{m-1}\}$. Obviously $\{e, a, a^2, \ldots, a^{m-1}\} \subseteq \langle a \rangle$. So

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\} = \{a, a^2, \ldots, a^m\}.$$

Suppose on the contrary that the elements $a, a^2, \ldots, a^m$ are not distinct. Then there exist $r, s \in \mathbb{N}$ such that $1 \leqslant s < r \leqslant m$ such that $a^s = a^r$. Then it is not difficult to show that $a^{r-s} = e$. But $r - s < m$, and this contradicts the minimality of $m$. ◯

EXAMPLES. (1) Consider the group $(\mathbb{Z}_8, +)$. Then $\langle 6 \rangle = \{6, 4, 2, 0\}$.

(2) Consider the multiplicative group $\mathcal{M}^*_{2,2}(\mathbb{R})$ of invertible matrices with real entries. Then

$$\left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

(3) Consider the subgroup $\langle 3 \rangle$ of $(\mathbb{R} \setminus \{0\}, \cdot)$. Then it is clear that $3 < 3^2 < 3^3 < \ldots$, so that $3^n \neq 1$ for any $n \in \mathbb{N}$. It follows that $\langle 3 \rangle$ is an infinite subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$.

Subgroups can also sometimes be obtained by imposing extra conditions.

PROPOSITION 1.9. *Suppose that $(G, *)$ is a group, and that $a \in G$. Suppose further that*

$$H = \{x \in G : a * x = x * a\}.$$

*Then $H$ is a subgroup of $G$.*

PROOF. Clearly $H$ is non-empty. Suppose that $x, y \in H$. Then $a * x = x * a$ and $a * y = y * a$. It follows that $(y' * a) * y = y' * (a * y) = y' * (y * a) = (y' * y) * a = a$. It is not difficult to deduce that $y' * a = a * y'$. Then $a * (x * y') = (a * x) * y' = (x * a) * y' = x * (a * y') = x * (y' * a) = (x * y') * a$, so that $x * y' \in H$. The result now follows from Theorem 1.5. ◯

PROPOSITION 1.10. *Suppose that $(G, *)$ is a group. Then*

$$Z(G) = \{x \in G : a * x = x * a \text{ for every } a \in G\}$$

*is a subgroup of $G$.*

PROOF. Clearly $H$ is non-empty, since $e \in H$. Suppose that $x, y \in H$. Then $a * x = x * a$ and $a * y = y * a$ for every $a \in G$. It follows that $(y' * a) * y = y' * (a * y) = y' * (y * a) = (y' * y) * a = a$ for every $a \in G$. It is not difficult to deduce that $y' * a = a * y'$ for every $a \in G$. Then

$$a * (x * y') = (a * x) * y' = (x * a) * y' = x * (a * y') = x * (y' * a) = (x * y') * a$$

for every $a \in G$, so that $x * y' \in H$. The result now follows from Theorem 1.5. ◯

DEFINITION. The group $Z(G)$ is called the centre of the group $G$.

REMARK. Note that $Z(G)$ contains precisely those elements of $G$ which commute with all elements of $G$.

## Problems for Chapter 1

1. Consider the set $\mathbb{R}$ of all real numbers. Define an operation $*$ on $\mathbb{R}$ as follows. For every $x, y \in \mathbb{R}$, let $x * y = x + y + 1$. Show that $(\mathbb{R}, *)$ forms an abelian group.

2. Let $G = \{(x, y) : x, y \in \mathbb{R} \setminus \{0\}\}$. Define an operation $*$ on $\mathbb{R}$ as follows. For $(x, y), (u, v) \in G$, let $(x, y) * (u, v) = (xu, yv)$. Show that $(\mathbb{R}, *)$ forms an abelian group.

3. Describe the following subgroups:
   (i) $\langle 1 \rangle$ in $(\mathbb{R}, +)$
   (ii) $\langle 1 \rangle$ in $(\mathbb{R} \setminus \{0\}, \cdot)$
   (iii) $\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$ in the multiplicative group $\mathcal{M}^*_{2,2}(\mathbb{R})$

4. Let $H$ denote the set of all positive real numbers. Is $H$ a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$? Justify your assertion.

5. Suppose that $(G, *)$ is a group, and that $G$ contains precisely 3 elements. Prove that $G$ is abelian.

6. Suppose that $(G, *)$ is a group, and that $G$ contains precisely 4 elements. Prove that $G$ is abelian. [*Hint*: Construct the group tables.]

7. Suppose that $(G, *)$ is an abelian group, and that $H$ and $K$ are subgroups of $G$. Prove that
$$H * K = \{h * k : h \in H \wedge k \in K\}$$
is a subgroup of $G$.

8. Suppose that $(G, *)$ is a group, and that $H = \{x \in G : x * x = e\}$.
   (i) Suppose further that $(G, *)$ is abelian. Prove that $H$ is a subgroup of $G$.
   (ii) Does the same result hold if $(G, *)$ is not abelian? Justify your assertion.

9. Suppose that $H$ and $K$ are subgroups of a group $G$.
   (i) Prove that $H \cap K$ is a subgroup of $G$.
   (ii) Is $H \cup K$ a subgroup of $G$? Justify your assertion.