MISCELLANEOUS TOPICS IN FIRST YEAR MATHEMATICS

W W L CHEN

 \bigodot W W L Chen, 1994, 2008.

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.

Chapter 4

INTRODUCTION TO GROUP THEORY

4.1. Some Examples

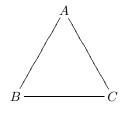
EXAMPLE 4.1.1. Consider the set \mathbb{Z} of integers and the operation addition. We take the following for granted:

- (1) For every $x, y \in \mathbb{Z}, x + y \in \mathbb{Z}$.
- (2) For every $x, y, z \in \mathbb{Z}$, (x+y) + z = x + (y+z).
- (3) For every $x \in \mathbb{Z}$, x + 0 = 0 + x = x.
- (4) For every $x \in \mathbb{Z}$, x + (-x) = (-x) + x = 0.

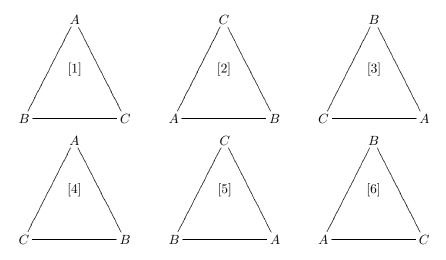
EXAMPLE 4.1.2. Consider now the set $\mathbb{R} \setminus \{0\}$ of non-zero real numbers and the operation multiplication. We take the following for granted:

- (1) For every $x, y \in \mathbb{R} \setminus \{0\}, xy \in \mathbb{R} \setminus \{0\}$.
- (2) For every $x, y, z \in \mathbb{R} \setminus \{0\}, (xy)z = x(yz)$.
- (3) For every $x \in \mathbb{R} \setminus \{0\}, x1 = 1x = x$.
- (4) For every $x \in \mathbb{R} \setminus \{0\}, xx^{-1} = x^{-1}x = 1$.

EXAMPLE 4.1.3. Let us consider an equilaterial triangle and label its corners A, B and C, and place it as follows:



If we cut it out and replace it in the same hole, we may end up with any one of the following six configurations:



Note that [2] and [3] are obtained from [1] by rotating anticlockwise about the centre by 120° and 240° respectively, while [4], [5] and [6] are obtained from [1], [2] and [3] respectively by reflecting across the vertical axis of symmetry. Let ρ denote an anticlockwise rotation by 120° and let ϕ denote a reflection across the vertical axis of symmetry. Then the six configurations correspond to the actions

$$e, \rho, \rho^2, \phi, \rho\phi, \rho^2\phi$$

respectively, where e denotes no change. Note also that $\phi \rho = \rho^2 \phi$. In fact, if we write

$$G = \{e, \rho, \rho^2, \phi, \rho\phi, \rho^2\phi\}$$

and combine the elements in the usual way, then it can be verified (with some hard work) that the following are true:

- (1) For every $x, y \in G, xy \in G$.
- (2) For every $x, y, z \in G$, (xy)z = x(yz).
- (3) For every $x \in G$, xe = ex = x.
- (4) For every $x \in G$, there exists $x' \in G$ such that xx' = x'x = e.

4.2. Formal Definition

There are many more examples of sets and operations where properties analogous to (1)-(4) in the previous section hold. 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.

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.

EXAMPLE 4.2.1. $(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\{0\}, +)$ and $(\{\pm 1\}, \cdot)$ are all groups.

EXAMPLE 4.2.2. The set \mathbb{R} , together with multiplication, does not form a group. The element 0 has no inverse.

Chapter 4 : Introduction to Group Theory

EXAMPLE 4.2.3. Consider the set $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ of integers modulo 5. Using the group table (addition modulo 5) below, it is not difficult to check that conditions (G1)–(G4) are all satisfied:

+	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

EXAMPLE 4.2.4. 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.

EXAMPLE 4.2.5. The set $\mathcal{M}_{2,2}(\mathbb{R})$ of 2×2 matrices with entries in \mathbb{R} , together with matrix addition, forms a group with identity $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

EXAMPLE 4.2.6. The set $\mathcal{M}_{2,2}^*(\mathbb{R})$ of invertible 2×2 matrices with entries in \mathbb{R} , together with matrix multiplication, forms a group with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

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 other words, if f and g are functions, 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.

REMARK. Note that all the groups in Examples 4.2.1 and 4.2.3–4.2.5 are abelian, while the group in Example 4.2.6 is not.

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

PROPOSITION 4A. Suppose that (G, *) is a group, and that $a, x, y \in G$. Then (a) (LEFT CANCELLATION) if a * x = a * y, then x = y; (b) (RIGHT CANCELLATION) if x * a = y * a, then x = y.

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

$$a' * (a * x) = a' * (a * y). \tag{1}$$

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

$$a' * (a * x) = (a' * a) * x = e * x = x.$$
(2)

Similarly

$$a' \ast (a \ast y) = y. \tag{3}$$

The result now follows on combining (1)-(3).

(b) can be proved in a similar way. \bigcirc

PROPOSITION 4B. 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 of G, then we must have $e_1 = e_1 * e_2 = e_2$. \bigcirc

PROPOSITION 4C. 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,

 $(y' * x') * (x * y) = \dots = e$ and $(x * y) * (y' * x') = \dots = e$,

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. \bigcirc

4.3. 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 $(\{\pm 1\}, \cdot)$. Clearly $\{0\} \subset \mathbb{Z}$ and $\{\pm 1\} \subset \mathbb{R} \setminus \{0\}$. We can therefore say that $(\{0\}, +)$ "is smaller than" $(\mathbb{Z}, +)$, and that $(\{\pm 1\}, \cdot)$ "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.

EXAMPLE 4.3.1. ($\{0\}, +$) is a subgroup of ($\mathbb{Z}, +$).

EXAMPLE 4.3.2. $(\{\pm 1\}, \cdot)$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$.

EXAMPLE 4.3.3. 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 $(\mathbb{Z}_8, +)$.

EXAMPLE 4.3.4. $(\mathbb{Z}_8, +)$ 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.

EXAMPLE 4.3.5. 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.

PROPOSITION 4D. 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. We need to check the following:

- (H1) For every $x, y \in H, x * y \in H$.
- (H2) For every $x, y, z \in H$, (x * y) * z = x * (y * z).
- (H3) There exists $e \in H$ such that x * e = e * x = x for every $x \in H$.
- (H4) For every $x \in H$, there exists an element $x' \in H$ such that x * x' = x' * x = e.

Note that (H1) is (S2). Next, note that (H2) is weaker than (G2). (H3) follows from (G3) and (S1). Finally (H4) follows from (G4) and (S3). \bigcirc

EXAMPLE 4.3.6. Let $H = \{3n : n \in \mathbb{Z}\}$. Then (H, +) is a subgroup of $(\mathbb{Z}, +)$.

EXAMPLE 4.3.7. Let $H = \{2^n : n \in \mathbb{Z}\}$. Then (H, \cdot) is a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$.

It is often convenient to use multiplicative notation to describe the binary operation *; in other words, 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 $x^{n+1} = x^n x$ and $x^{-n} = (x')^n$. Then it is not difficult to prove that for every $m, n \in \mathbb{Z}$, we have $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$.

REMARK. Suppose that x and y are elements of a group. It is not always true that $(xy)^n = x^n y^n$. 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.

A very special type of subgroups are obtained by building from a particular element of the group.

PROPOSITION 4E. Suppose that (G, *) is a group, and that $a \in G$. Then $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

PROOF. Clearly $e = a^0 \in \langle a \rangle$. 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 $m + n \in \mathbb{Z}$. Also, note that $x * a^{-m} = a^m a^{-m} = e$ and $a^{-m} * x = a^{-m} a^m = e$, so that $x' = a^{-m} \in \langle a \rangle$. The result now follows from Proposition 4D. \bigcirc

DEFINITION. We say that the group $\langle a \rangle$ in Proposition 4E is the cyclic subgroup of G generated by the element a.

PROPOSITION 4F. 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 $n \geq 2$. 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 $n \in \mathbb{Z}$. \bigcirc

EXAMPLE 4.3.8. Consider the subgroup $\langle 4 \rangle$ of $(\mathbb{Z}, +)$. Note that $4^2 = 4 + 4$ and that $4^{-3} = (-4) + (-4) + (-4)$. Hence $\langle 4 \rangle = \{4n : n \in \mathbb{Z}\}$.

PROPOSITION 4G. Suppose that (G, *) is a group with identity element e, and that $a \in G$. Then exactly one of the following is true:

- (a) 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.
- (b) There exists a smallest $m \in \mathbb{N}$ such that $\langle a \rangle = \{a, a^2, \dots, a^m\}$.

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

(a) 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.

(b) 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 $0 \le r < m$. 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 $1 \le s < r \le m$ 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. \bigcirc

EXAMPLE 4.3.9. Consider the group $(\mathbb{Z}_8, +)$. Then $\langle 6 \rangle = \{6, 4, 2, 0\}$.

EXAMPLE 4.3.10. Consider the multiplicative group $\mathcal{M}_{2,2}^*(\mathbb{R})$ of invertible matrices with real entries. Then

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

EXAMPLE 4.3.11. 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 $(\mathbb{R} \setminus \{0\}, \cdot)$.

4.4. Order

DEFINITION. Suppose that a group G has a finite number of elements. Then we say that G is a finite group, and the number of elements G, denoted by |G|, is called the order of the group G. Also, we say that G is an infinite group if the number of elements of G is infinite.

EXAMPLE 4.4.1. If $G = \mathbb{Z}_8$, with addition modulo 8, then |G| = 8.

EXAMPLE 4.4.2. The group $(\mathbb{Z}, +)$ is infinite.

DEFINITION. Suppose that G is a group, and that $a \in G$. Suppose further that $\langle a \rangle$ is finite. Then we say that the order of a is $|\langle a \rangle|$. On the other hand, if $\langle a \rangle$ is infinite, then we say that a is of infinite order.

REMARK. If $\langle a \rangle$ is finite, then it can be shown that the order of a is the smallest natural number $n \in \mathbb{N}$ such that $a^n = e$.

EXAMPLE 4.4.3. In $(\mathbb{Z}_8, +)$, the elements 1, 3, 5 and 7 are all of order 8, the elements 2 and 6 have order 4, the element 4 has order 2 and the element 0 has order 1.

EXAMPLE 4.4.4. Is there an element of finite order in $(\mathbb{Z}, +)$?

Note that in Example 4.4.1, the order of each element of $(\mathbb{Z}_8, +)$ is a divisor of the order of $(\mathbb{Z}_8, +)$. This turns out to be the case whenever the group in question is finite. In Section 4.6, we shall establish the following important result.

PROPOSITION 4H. (LAGRANGE'S THEOREM) Suppose that G is a finite group, and that H is a subgroup of G. Then |H| divides |G|.

PROPOSITION 4J. Suppose that G is a finite group, and that $a \in G$. Then the order of a divides |G|.

PROOF. Simply note that the order of a is the order of $\langle a \rangle$. On the other hand, $\langle a \rangle$ is a subgroup of G by Proposition 4E. The result now follows from Proposition 4H. \bigcirc

4.5. Cyclic Groups

DEFINITION. A group G is said to be cyclic if there exists $a \in G$ such that $G = \langle a \rangle$.

EXAMPLE 4.5.1. $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle.$

EXAMPLE 4.5.2. $(\{\pm 1\}, \cdot) = \langle -1 \rangle$.

EXAMPLE 4.5.3. $(\mathbb{Z}, +) = \langle 1 \rangle$.

EXAMPLE 4.5.4. $(\mathbb{R} \setminus \{0\}, \cdot)$ is not cyclic. For take any $a \in \mathbb{R} \setminus \{0\}$. Then clearly $|a|^{1/2} \in \mathbb{R} \setminus \{0\}$ but $|a|^{1/2} \notin \langle a \rangle$. It follows that $(\mathbb{R} \setminus \{0\}, \cdot) \neq \langle a \rangle$ for any $a \in \mathbb{R}$.

PROPOSITION 4K. Suppose that G is a group of order p, where p is a prime. Then G is cyclic.

PROOF. Let $a \in G$ such that $a \neq e$. Then $\langle a \rangle \neq \{e\}$, so that $|\langle a \rangle| \neq 1$. On the other hand, $\langle a \rangle$ is a subgroup of G by Proposition 4E, and so $|\langle a \rangle|$ divides p by Proposition 4H. It follows that $\langle a \rangle = G$. \bigcirc

PROPOSITION 4L. A finite group G is cyclic if and only if G contains an element of order |G|.

PROOF. Let $a \in G$ be of order |G| = n. Then $a, a^2, \ldots, a^n \in G$ are distinct, so that

$$G = \{a, a^2, \dots, a^n\} \subseteq \langle a \rangle.$$

Hence $G = \langle a \rangle$. On the other hand, if G does not contain any element of order |G|, then for every $x \in G$, $\langle x \rangle = \{x, x^2, \ldots, x^m\}$ for some $m \in \mathbb{N}$ where m is a proper divisor of |G| by Proposition 4J, so that m < |G|. It follows that $\langle x \rangle \neq G$. Hence G is not cyclic. \bigcirc

PROPOSITION 4M. Suppose that G is a cyclic group. Then G is abelian.

PROOF. Let $a \in G$ such that $G = \langle a \rangle$. Then for every $x, y \in G$, there exist $m, n \in \mathbb{Z}$ such that $x = a^m$ and $y = a^n$. It follows that $x * y = a^m a^n = a^{m+n} = a^n a^m = y * x$. Hence G is abelian. \bigcirc

We complete this section by establishing the following result concerning subgroups of cyclic groups.

PROPOSITION 4N. Suppose that G is a cyclic group, and that H is a subgroup of G. Then H is cyclic.

PROOF. Let $a \in G$ such that $G = \langle a \rangle$. There clearly exists $m \in \mathbb{N}$ such that

$$a^m \in H$$
 and $a, a^2, a^3, \dots, a^{m-1} \notin H$.

We shall show that $H = \langle a^m \rangle$. Note first of all that by Proposition 4F, we have $\langle a^m \rangle \subseteq H$. It remains to show that $H \subseteq \langle a^m \rangle$. Suppose on the contrary that this is not the case. Then there exists $c \in \mathbb{Z}$ such that $m \nmid c$ and $a^c \in H$. By Proposition 3A, there exist $q, r \in \mathbb{Z}$ such that c = mq + r and $0 \leq r < m$. Furthermore, we have $1 \leq r < m$ since $m \nmid c$. It follows that $a^r = a^{c-mq} = a^c (a^{-m})^q \in H$, clearly a contradiction. \bigcirc

4.6. Further Discussion

In this section, we shall establish Langrage's theorem. Our idea is to partition the finite group G into a disjoint union of a number of sets, each of which having the same number of elements as the given subgroup H. Naturally, the subgroup H is used to construct these sets.

DEFINITION. Suppose that H is a subgroup of a group G. For every element $x \in G$, the set

$$xH = \{xh : h \in H\}$$

is called a left coset of H in G.

PROPOSITION 4P. Suppose that H is a subgroup of a group G. Then for every $x, y \in G$, we have xH = yH if and only if $x^{-1}y \in H$.

Chapter 4 : Introduction to Group Theory

PROOF. (\Rightarrow) Suppose that xH = yH. Since $e \in H$, it follows that $y \in xH$, so that y = xh for some $h \in H$. Note now that $x^{-1}y = h$ in this case.

(⇐) Suppose that $x^{-1}y = h \in H$. Then y = xh, so that yH = xhH. It is not difficult to show that hH = H, so that xhH = xH. \bigcirc

PROPOSITION 4Q. Suppose that H is a subgroup of a group G. Then for every $x, y \in G$, either xH = yH or $xH \cap yH = \emptyset$. In other words, the left cosets are either identical or disjoint.

PROOF. Suppose that $xH \cap yH \neq \emptyset$. Let $z \in xH \cap yH$. Then there exist $h_1, h_2 \in H$ such that $z = xh_1 = yh_2$, so that $x^{-1}y = h_1h_2^{-1} \in H$. It follows from Proposition 4P that xH = yH. \bigcirc

PROOF OF PROPOSITION 4H. Suppose that G is a finite group. Then every subgroup H is finite. Suppose that $H = \{h_1, \ldots, h_k\}$. Then in view of Proposition 4A(a), any left coset $xH = \{xh_1, \ldots, xh_k\}$ contains k distinct elements. It follows that all the left cosets have the same number of elements as H. On the other hand, every $x \in G$ satisfies $x \in xH$ and so belongs to some left coset. In view of Proposition 4Q, we now conclude that G must be the disjoint union of a finite number of left cosets. It follows that |H| must divide |G|. \bigcirc

4.7. Groups of Small Order

For the remainder of this chapter, we shall construct all groups of order up to 7.

First of all, note that there is exactly one group (G, *) of order 1. By (G3), the only possibility is $G = \{e\}$, where e is the identity element. Secondly, note that if (G, *) is of prime order, then it follows from Proposition 4K that it is cyclic. It follows that the only groups of order 2, 3, 5 or 7 are cyclic groups. It remains to construct groups of order 4 and 6. We shall use multiplicative notation, and omit reference to *.

Suppose that G is a group of order 4. Write $G = \{e, a, b, c\}$. By Proposition 4J, the order of the elements of G are 1, 2 or 4. Clearly the only element of order 1 is e.

(1) Suppose that G has an element of order 4. Then by Proposition 4L, G is cyclic.

(2) Suppose that G has no element of order 4. Then a, b and c must all have order 2, so that aa = bb = cc = e. On the other hand, note that

 $ab \begin{cases} \neq e, & \text{otherwise } ab = aa, \text{ so that } b = a, \\ \neq a, & \text{otherwise } ab = ae, \text{ so that } b = e, \\ \neq b, & \text{otherwise } ab = eb, \text{ so that } a = e. \end{cases}$

Hence we must have ab = c. Similarly ba = c. Similar arguments give ac = ca = b and bc = cb = a. We must therefore have the group table below:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

It follows that there are essentially two groups of order 4.

Suppose next that G is a group of order 6. Write $G = \{e, a, b, c, s, t\}$. By Proposition 4J, the order of the elements of G are 1, 2, 3 or 6. Clearly the only element of order 1 is e.

(1) Suppose that G has an element of order 6. Then by Proposition 4L, G is cyclic.

(2) Suppose that G has no element of order 6 but has an element of order 3. Without loss of generality, assume that s is of order 3, and write $t = s^2$. Then $G = \{e, a, b, c, s, s^2\}$. We have the following partial group table:

	e	a	b	с	s	s^2
e	e	a	b	c	s	s^2
a	a					
b	b					
c	c					
s	s				s^2	e
s^2	s^2				e	s

The three elements a, b and c are of order 2 or 3. Suppose that one of these, c say, is of order 3. Let us consider c^2 . Firstly, $c^2 \neq s$, for otherwise $cs = c^3 = e = s^2s$, so that $c = s^2$. Secondly $c^2 \neq s^2$, for otherwise $cs^2 = c^3 = e = ss^2$, so that c = s. Furthermore $c^2 \neq e$ (why?) and $c^2 \neq c$ (why?). Without loss of generality, we may therefore assume that $c^2 = b$. Note now that s and s^2 are inverses of each other, and that c and $c^2 = b$ are inverses of each other. Since e is its own inverse, the inverse of a must be a, so that $a^2 = e$. We have therefore shown that at least one of the three elements a, b and c must have order 2. Without loss of generality, we assume that $a^2 = e$. Then we have $G = \{e, a, b, c, s, s^2\}$, with $s^3 = e$ and $a^2 = e$. Note now that

$$sa\begin{cases} \neq e, & \text{otherwise } sa = aa, \text{ so that } s = a, \\ \neq a, & \text{otherwise } sa = ea, \text{ so that } s = e, \\ \neq s, & \text{otherwise } sa = se, \text{ so that } a = e, \\ \neq s^2, & \text{otherwise } sa = ss, \text{ so that } a = s. \end{cases}$$

Without loss of generality, let sa = b. Now

$$as \begin{cases} \neq e, & \text{otherwise } as = aa, \text{ so that } s = a, \\ \neq a, & \text{otherwise } as = ae, \text{ so that } s = e, \\ \neq s, & \text{otherwise } as = es, \text{ so that } a = e, \\ \neq s^2, & \text{otherwise } as = ss, \text{ so that } a = s. \end{cases}$$

Furthermore, $as \neq b$, for otherwise sa = b = as, so that $b^2 = saas = ses = s^2$, whence b is not of order 2. Hence b is of order 3, and so $bs^2 = b^3 = e = ss^2$, giving b = s. It follows that as = c. We have the following partial group table:

	e	a	b	c	s	s^2
e	e	a	b	c	s	s^2
a	a	e			c	
b	b					
c	c					
s	s	b			s^2	e
s^2	s^2				e	s

Now consider sc. From the table, sc cannot be equal to s, b, s^2 or e (why?). Also $sc \neq c$ (why?). Hence sc = a. This forces sb = c (why?). Similarly bs = a and cs = b. We have the following partial group table:

	e	a	b	c	s	s^2
e	e	a	b	c	s	s^2
a	a	e			c	
b	b				a	
c	c				b	
s	s	b	c	a	s^2	e
s^2	s^2				e	s

Next, we can complete the last row and the last column. For example, $s^2a = ssa = sb = c$. Similarly $s^2b = a$ and $s^2c = b$. Also, $as^2 = ass = cs = b$. Similarly $bs^2 = c$ and $cs^2 = a$. On the other hand, we have already shown earlier than $b^2 \neq s^2$. Suppose now that $b^2 = s$. Then b is not of order 2. Also, $b^3 = bs = a$, so that b is not of order 3. Hence $b^2 \neq s$, and so we must have $b^2 = e$. Similarly $c^2 = e$. We have the following partial group table:

	e	a	b	c	s	s^2
e	e	a	b	c	s	s^2
a	a	e			c	b
b	b		e		a	с
c	c			e	b	a
s	s	b	c	a	s^2	e
s^2	s^2	c	a	b	e	s

We can now complete the table in the following way. Note that $ab = sccs = ses = s^2$ and so ac = s. It follows that we must have $bc = s^2$, ba = s, $ca = s^2$ and cb = s. We now have the following group table (it can indeed be checked that it is a group):

	e	a	b	c	s	s^2
e	e	a	b	c	s	s^2
a	a	e	s^2	s	c	b
b	b	s	e	s^2	a	с
c	c	s^2	s	e	b	a
s	s	b	c	a	s^2	e
s^2	s^2	с	a	b	e	s

Note that the group is non-abelian.

(3) Suppose that G has no element of order 3 or 6. Then $a^2 = b^2 = c^2 = s^2 = t^2 = e$ (the reader should start a partial group table). Note that $ab \neq e, a, b$, so we may assume, without loss of generality, that ab = c. Then ac = aab = eb = b. It follows that $as \neq e, a, b, c, s$, so that as = t, forcing at = aas = es = s. Next, note that bac = bb = e = cc, so that ba = c, forcing bc = bba = ea = a. We now arrive at the absurd situation that $bs \neq e, a, b, c, s, t$. It follows that no such group G exists.

We can now conclude that there are essentially two groups of order 6. Note that the non-abelian group of order 6 is the group first described in Example 4.1.1.

PROBLEMS FOR CHAPTER 4

- 1. Show that the set of all positive real numbers forms a group under multiplication.
- 2. Let $G = \mathbb{Z}$, and write x * y = x + y 4 for every $x, y \in G$. Show that (G, *) is a group.
- 3. Let G denote the set of all odd integers. Does G form a group under multiplication of integers?
- 4. Verify that the set

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \right\}$$

forms a group under multiplication of matrices. Is this group abelian?

5. Let S denote the set of all non-zero real numbers. Consider the set $A = \{f_1, f_2, f_3, f_4\}$ of the four functions

$$f_1:S \to S: x \mapsto x, \quad f_2:S \to S: x \mapsto -x, \quad f_3:S \to S: x \mapsto 1/x, \quad f_4:S \to S: x \mapsto -1/x.$$

Show that A forms a group under composition of functions. Is A abelian? Is A cyclic?

- 6. Let (G, *) be a group such that x * x = e for every $x \in G$. Show that (G, *) is abelian. [HINT: Let $x, y \in G$. Consider x * y * x * y and x * y * y * x.]
- 7. Show that a group of order 3 must be abelian.
- 8. Suppose that H and K are both subgroups of a group G.
 - a) Prove that $H \cap K$ is a subgroup of G.
 - b) Suppose further that |H| and |K| are both finite but relatively prime. Explain why $H \cap K = \{e\}$.

b) $\langle 1 \rangle$ in $(\mathbb{R} \setminus \{0\}, \cdot)$

- 9. Find each of the following subgroups:
 a) ⟨1⟩ in (ℝ, +)
- 10. Consider the set $G = \{(x_1, x_2, x_3) : x_1, x_2, x_3 \in \{0, 1\}\}$. Define an operation * on G by writing

 $(x_1, x_2, x_3) * (y_1, y_2, y_3) = (x_1 \circ y_1, x_2 \circ y_2, x_3 \circ y_3),$

where $0 \circ 0 = 0$, $0 \circ 1 = 1$, $1 \circ 0 = 1$, and $1 \circ 1 = 0$.

- a) Convince yourself that (G, *) is a group of order 8.
- b) What is the identity element of (G, *)?
- c) Show that every non-identity element in (G, *) is of order 2.
- d) Explain why (G, *) is not cyclic.
- 11. How many groups of order 8 can you construct?