# MISCELLANEOUS TOPICS IN FIRST YEAR MATHEMATICS 

W W L CHEN

(C) 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.

## 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 $\mathbb{R} \backslash\{0\}$ of non-zero real numbers and the operation multiplication. We take the following for granted:
(1) For every $x, y \in \mathbb{R} \backslash\{0\}, x y \in \mathbb{R} \backslash\{0\}$.
(2) For every $x, y, z \in \mathbb{R} \backslash\{0\},(x y) z=x(y z)$.
(3) For every $x \in \mathbb{R} \backslash\{0\}, x 1=1 x=x$.
(4) For every $x \in \mathbb{R} \backslash\{0\}, x x^{-1}=x^{-1} x=1$.

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 $120^{\circ}$ and $240^{\circ}$ respectively, while [4], [5] and [6] are obtained from [1], [2] and [3] respectively by reflecting across the vertical axis of symmetry. Let $\rho$ denote an anticlockwise rotation by $120^{\circ}$ and let $\phi$ denote a reflection across the vertical axis of symmetry. Then the six configurations correspond to the actions

$$
e, \quad \rho, \quad \rho^{2}, \quad \phi, \quad \rho \phi, \quad \rho^{2} \phi
$$

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

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

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 $x, y \in G, x y \in G$.
(2) For every $x, y, z \in G,(x y) z=x(y z)$.
(3) For every $x \in G, x e=e x=x$.
(4) For every $x \in G$, there exists $x^{\prime} \in G$ such that $x x^{\prime}=x^{\prime} x=e$.

### 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 $x^{\prime} \in G$ such that $x * x^{\prime}=x^{\prime} * x=e$.
Remark. Sometimes we omit reference to the operation $*$ and simply refer to a group $G$.
Example 4.2.1. $(\mathbb{Z},+),(\mathbb{R} \backslash\{0\}, \cdot),(\{0\},+)$ 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.

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 $\mathbb{Z}_{n}=\{0,1,2, \ldots, n-1\}$ of integers modulo $n$ forms a group under addition modulo $n$.

Example 4.2.5. The set $\mathcal{M}_{2,2}(\mathbb{R})$ of $2 \times 2$ matrices with entries in $\mathbb{R}$, together with matrix addition, forms a group with identity $\left(\begin{array}{ll}0 & 0 \\ 0 & 0\end{array}\right)$.

Example 4.2.6. 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 $\left(\begin{array}{ll}1 & 0 \\ 0 & 1\end{array}\right)$.

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 $A B=B A$. 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 $a^{\prime} \in G$ by (G4) and

$$
\begin{equation*}
a^{\prime} *(a * x)=a^{\prime} *(a * y) . \tag{1}
\end{equation*}
$$

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

$$
\begin{equation*}
a^{\prime} *(a * x)=\left(a^{\prime} * a\right) * x=e * x=x \tag{2}
\end{equation*}
$$

Similarly

$$
\begin{equation*}
a^{\prime} *(a * y)=y \tag{3}
\end{equation*}
$$

The result now follows on combining (1)-(3).
(b) can be proved in a similar way.

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 $e_{1}=e_{1} * e_{2}=e_{2}$.

PROPOSITION 4C. Suppose that $(G, *)$ is a group, and that $x \in G$. Then the inverse element $x^{\prime}$ is unique. On the other hand, for every $x, y \in G$, we have $(x * y)^{\prime}=y^{\prime} * x^{\prime}$.

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,

$$
\left(y^{\prime} * x^{\prime}\right) *(x * y)=\ldots=e \quad \text { and } \quad(x * y) *\left(y^{\prime} * x^{\prime}\right)=\ldots=e
$$

so that $y^{\prime} * x^{\prime}$ satisfies the requirements for being the inverse of $x * y$. It follows that $(x * y)^{\prime}=y^{\prime} * x^{\prime}$ by the uniqueness of inverse.

### 4.3. Subgroups

Recall that $(\mathbb{Z},+)$ forms a group, and so does $(\{0\},+)$. Another example is that $(\mathbb{R} \backslash\{0\}, \cdot)$ forms a group, and so does $(\{ \pm 1\}, \cdot)$. Clearly $\{0\} \subset \mathbb{Z}$ and $\{ \pm 1\} \subset \mathbb{R} \backslash\{0\}$. We can therefore say that $(\{0\},+)$ "is smaller than" $(\mathbb{Z},+)$, and that $(\{ \pm 1\}, \cdot)$ "is smaller than" $(\mathbb{R} \backslash\{0\}, \cdot)$.

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 $(\mathbb{R} \backslash\{0\}, \cdot)$.
Example 4.3.3. Consider the group $\left(\mathbb{Z}_{8},+\right)$, where + denotes addition modulo 8. If $H=\{0,2,4,6\}$, then $(H,+)$, where + again denotes addition modulo 8 , is a subgroup of $\left(\mathbb{Z}_{8},+\right)$.

Example 4.3.4. $\left(\mathbb{Z}_{8},+\right)$ forms a group. $\left(\mathbb{Z}_{4},+\right)$ 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 $\left(\mathbb{Z}_{4},+\right)$ is a subgroup of $\left(\mathbb{Z}_{8},+\right)$. 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 $x \in H, x^{\prime} \in H$.
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 $x^{\prime} \in H$ such that $x * x^{\prime}=x^{\prime} * x=e$.

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).

Example 4.3.6. Let $H=\{3 n: n \in \mathbb{Z}\}$. Then $(H,+)$ is a subgroup of $(\mathbb{Z},+)$.
Example 4.3.7. Let $H=\left\{2^{n}: n \in \mathbb{Z}\right\}$. Then $(H, \cdot)$ is a subgroup of $(\mathbb{R} \backslash\{0\}, \cdot)$.
It is often convenient to use multiplicative notation to describe the binary operation $*$; in other words, we write $x y$ 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 $x^{-n}=\left(x^{\prime}\right)^{n}$. 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 $\left(x^{m}\right)^{n}=x^{m n}$.

Remark. Suppose that $x$ and $y$ are elements of a group. It is not always true that $(x y)^{n}=x^{n} y^{n}$. 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 $\langle a\rangle=\left\{a^{n}: n \in \mathbb{Z}\right\}$ 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 $x^{\prime}=a^{-m} \in\langle a\rangle$. The result now follows from Proposition 4D.

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 $a^{2}=a a, \ldots, a^{n}=a^{n-1} a$, 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 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 $\langle 4\rangle=\{4 n: n \in \mathbb{Z}\}$.

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 $\langle a\rangle=\left\{a, a^{2}, \ldots, a^{m}\right\}$.

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 $a^{m-n}=a^{m} a^{-n}=a^{m}\left(a^{n}\right)^{\prime}=a^{m}\left(a^{m}\right)^{\prime}=e$, a contradiction.
(b) Consider the set $S=\left\{n \in \mathbb{N}: a^{n}=e\right\}$. 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 $n=m q+r$, where $q, r \in \mathbb{Z}$ and $0 \leq r<m$. Then $a^{n}=a^{m q} a^{r}=\left(a^{m}\right)^{q} a^{r}=e^{q} a^{r}=a^{r}$, so clearly $\langle a\rangle \subseteq\left\{e, a, a^{2}, \ldots, a^{m-1}\right\}$. Obviously $\left\{e, a, a^{2}, \ldots, a^{m-1}\right\} \subseteq\langle a\rangle$. So $\langle a\rangle=\left\{e, a, a^{2}, \ldots, a^{m-1}\right\}=\left\{a, a^{2}, \ldots, a^{m}\right\}$. 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 $1 \leq s<r \leq m$ 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 $m$.

Example 4.3.9. Consider the group $\left(\mathbb{Z}_{8},+\right)$. 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

$$
\left\langle\left(\begin{array}{cc}
0 & 1 \\
-1 & 0
\end{array}\right)\right\rangle=\left\{\left(\begin{array}{cc}
0 & 1 \\
-1 & 0
\end{array}\right),\left(\begin{array}{cc}
-1 & 0 \\
0 & -1
\end{array}\right),\left(\begin{array}{cc}
0 & -1 \\
1 & 0
\end{array}\right),\left(\begin{array}{ll}
1 & 0 \\
0 & 1
\end{array}\right)\right\}
$$

Example 4.3.11. Consider the subgroup $\langle 3\rangle$ of $(\mathbb{R} \backslash\{0\}, \cdot)$. 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 $(\mathbb{R} \backslash\{0\}, \cdot)$.

### 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 $\left(\mathbb{Z}_{8},+\right)$, 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 $\left(\mathbb{Z}_{8},+\right)$ is a divisor of the order of $\left(\mathbb{Z}_{8},+\right)$. 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.

### 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. $\left(\mathbb{Z}_{8},+\right)=\langle 1\rangle=\langle 3\rangle=\langle 5\rangle=\langle 7\rangle$.
Example 4.5.2. $(\{ \pm 1\}, \cdot)=\langle-1\rangle$.

Example 4.5.3. $(\mathbb{Z},+)=\langle 1\rangle$.
Example 4.5.4. ( $\mathbb{R} \backslash\{0\}, \cdot)$ is not cyclic. For take any $a \in \mathbb{R} \backslash\{0\}$. Then clearly $|a|^{1 / 2} \in \mathbb{R} \backslash\{0\}$ but $|a|^{1 / 2} \notin\langle a\rangle$. It follows that $(\mathbb{R} \backslash\{0\}, \cdot) \neq\langle a\rangle$ 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 $\langle a\rangle=G$.

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

$$
G=\left\{a, a^{2}, \ldots, a^{n}\right\} \subseteq\langle a\rangle
$$

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

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.

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

$$
a^{m} \in H \quad \text { and } \quad a, a^{2}, a^{3}, \ldots, a^{m-1} \notin H
$$

We shall show that $H=\left\langle a^{m}\right\rangle$. Note first of all that by Proposition 4F, we have $\left\langle a^{m}\right\rangle \subseteq H$. It remains to show that $H \subseteq\left\langle a^{m}\right\rangle$. 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 $c=m q+r$ and $0 \leq r<m$. Furthermore, we have $1 \leq r<m$ since $m \nmid c$. It follows that $a^{r}=a^{c-m q}=a^{c}\left(a^{-m}\right)^{q} \in H$, clearly a contradiction.

### 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

$$
x H=\{x h: h \in H\}
$$

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 $x H=y H$ if and only if $x^{-1} y \in H$.

Proof. $(\Rightarrow)$ Suppose that $x H=y H$. Since $e \in H$, it follows that $y \in x H$, so that $y=x h$ for some $h \in H$. Note now that $x^{-1} y=h$ in this case.
$(\Leftarrow)$ Suppose that $x^{-1} y=h \in H$. Then $y=x h$, so that $y H=x h H$. It is not difficult to show that $h H=H$, so that $x h H=x H$.

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

Proof. Suppose that $x H \cap y H \neq \emptyset$. Let $z \in x H \cap y H$. Then there exist $h_{1}, h_{2} \in H$ such that $z=x h_{1}=y h_{2}$, so that $x^{-1} y=h_{1} h_{2}^{-1} \in H$. It follows from Proposition 4P that $x H=y H$.

Proof of Proposition 4H. Suppose that $G$ is a finite group. Then every subgroup $H$ is finite. Suppose that $H=\left\{h_{1}, \ldots, h_{k}\right\}$. Then in view of Proposition $4 \mathrm{~A}(\mathrm{a})$, any left coset $x H=\left\{x h_{1}, \ldots, x h_{k}\right\}$ 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 $x \in x H$ 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 4 K 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 $a a=b b=c c=e$. On the other hand, note that

$$
a b \begin{cases}\neq e, & \text { otherwise } a b=a a, \text { so that } b=a, \\ \neq a, & \text { otherwise } a b=a e, \text { so that } b=e \\ \neq b, & \text { otherwise } a b=e b, \text { so that } a=e\end{cases}
$$

Hence we must have $a b=c$. Similarly $b a=c$. Similar arguments give $a c=c a=b$ and $b c=c b=a$. 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 $G=\left\{e, a, b, c, s, s^{2}\right\}$. We have the following partial group table:

|  | $e$ | $a$ | $b$ | $c$ | $s$ | $s^{2}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $e$ | $e$ | $a$ | $b$ | $c$ | $s$ | $s^{2}$ |
| $a$ | $a$ |  |  |  |  |  |
| $b$ | $b$ |  |  |  |  |  |
| $c$ | $c$ |  |  |  |  |  |
| $s$ | $s$ |  |  |  | $s^{2}$ | $e$ |
| $s^{2}$ | $s^{2}$ |  |  |  | $e$ | $s$ |

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 $c s=c^{3}=e=s^{2} s$, so that $c=s^{2}$. Secondly $c^{2} \neq s^{2}$, for otherwise $c s^{2}=c^{3}=e=s s^{2}$, 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 $G=\left\{e, a, b, c, s, s^{2}\right\}$, with $s^{3}=e$ and $a^{2}=e$. Note now that

$$
s a \begin{cases}\neq e, & \text { otherwise } s a=a a, \text { so that } s=a, \\ \neq a, & \text { otherwise } s a=e a, \text { so that } s=e, \\ \neq s, & \text { otherwise } s a=s e, \text { so that } a=e, \\ \neq s^{2}, & \text { otherwise } s a=s s, \text { so that } a=s\end{cases}
$$

Without loss of generality, let $s a=b$. Now

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

Furthermore, $a s \neq b$, for otherwise $s a=b=a s$, so that $b^{2}=s a a s=s e s=s^{2}$, whence $b$ is not of order 2 . Hence $b$ is of order 3 , and so $b s^{2}=b^{3}=e=s s^{2}$, giving $b=s$. It follows that $a s=c$. 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 $s c$. From the table, $s c$ cannot be equal to $s, b, s^{2}$ or $e$ (why?). Also $s c \neq c$ (why?). Hence $s c=a$. This forces $s b=c$ (why?). Similarly $b s=a$ and $c s=b$. 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, $s^{2} a=s s a=s b=c$. Similarly $s^{2} b=a$ and $s^{2} c=b$. Also, $a s^{2}=a s s=c s=b$. Similarly $b s^{2}=c$ and $c s^{2}=a$. 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, $b^{3}=b s=a$, 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:

|  | $e$ | $a$ | $b$ | $c$ | $s$ | $s^{2}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $e$ | $e$ | $a$ | $b$ | $c$ | $s$ | $s^{2}$ |
| $a$ | $a$ | $e$ |  |  | $c$ | $b$ |
| $b$ | $b$ |  | $e$ |  | $a$ | $c$ |
| $c$ | $c$ |  |  | $e$ | $b$ | $a$ |
| $s$ | $s$ | $b$ | $c$ | $a$ | $s^{2}$ | $e$ |
| $s^{2}$ | $s^{2}$ | $c$ | $a$ | $b$ | $e$ | $s$ |

We can now complete the table in the following way. Note that $a b=s c c s=s e s=s^{2}$ and so $a c=s$. It follows that we must have $b c=s^{2}, b a=s, c a=s^{2}$ and $c b=s$. We now have the following group table (it can indeed be checked that it is a group):

|  | $e$ | $a$ | $b$ | $c$ | $s$ | $s^{2}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $e$ | $e$ | $a$ | $b$ | $c$ | $s$ | $s^{2}$ |
| $a$ | $a$ | $e$ | $s^{2}$ | $s$ | $c$ | $b$ |
| $b$ | $b$ | $s$ | $e$ | $s^{2}$ | $a$ | $c$ |
| $c$ | $c$ | $s^{2}$ | $s$ | $e$ | $b$ | $a$ |
| $s$ | $s$ | $b$ | $c$ | $a$ | $s^{2}$ | $e$ |
| $s^{2}$ | $s^{2}$ | $c$ | $a$ | $b$ | $e$ | $s$ |

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 $a b \neq e, a, b$, so we may assume, without loss of generality, that $a b=c$. Then $a c=a a b=e b=b$. It follows that $a s \neq e, a, b, c, s$, so that $a s=t$, forcing $a t=a a s=e s=s$. Next, note that $b a c=b b=e=c c$, so that $b a=c$, forcing $b c=b b a=e a=a$. We now arrive at the absurd situation that $b s \neq e, a, b, c, s, t$. 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

$$
G=\left\{\left(\begin{array}{ll}
1 & 0 \\
0 & 1
\end{array}\right),\left(\begin{array}{ll}
-1 & 1 \\
-1 & 0
\end{array}\right),\left(\begin{array}{cc}
0 & -1 \\
1 & -1
\end{array}\right),\left(\begin{array}{cc}
-1 & 0 \\
0 & -1
\end{array}\right),\left(\begin{array}{cc}
1 & -1 \\
1 & 0
\end{array}\right),\left(\begin{array}{cc}
0 & 1 \\
-1 & 1
\end{array}\right)\right\}
$$

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 $A=\left\{f_{1}, f_{2}, f_{3}, f_{4}\right\}$ of the four functions

$$
f_{1}: S \rightarrow S: x \mapsto x, \quad f_{2}: S \rightarrow S: x \mapsto-x, \quad f_{3}: S \rightarrow S: x \mapsto 1 / x, \quad f_{4}: S \rightarrow S: x \mapsto-1 / x
$$

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 $H \cap K=\{e\}$.
9. Find each of the following subgroups:
a) $\langle 1\rangle$ in $(\mathbb{R},+)$
b) $\langle 1\rangle$ in $(\mathbb{R} \backslash\{0\}, \cdot)$
10. Consider the set $G=\left\{\left(x_{1}, x_{2}, x_{3}\right): x_{1}, x_{2}, x_{3} \in\{0,1\}\right\}$. Define an operation $*$ on $G$ by writing

$$
\left(x_{1}, x_{2}, x_{3}\right) *\left(y_{1}, y_{2}, y_{3}\right)=\left(x_{1} \circ y_{1}, x_{2} \circ y_{2}, x_{3} \circ y_{3}\right),
$$

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?

