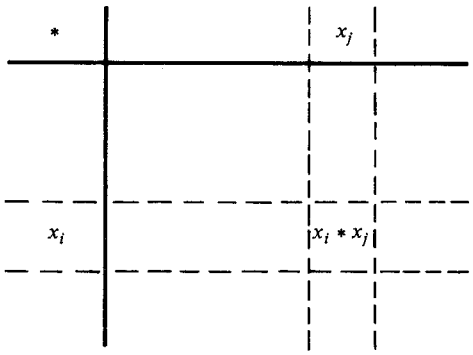
1: Groups

Abstract algebra is basically a study of sets with binary operations. A binary operation (or law of composition) on a set E is a mapping $f : E \times E \to E$ described variously by $(x, y) \to x * y$, $(x, y) \to x + y$, $(x, y) \to xy$, etc. When E is finite it is sometimes convenient to represent a binary operation on E by means of a Cayley table, the interpretation of which is that $x_i * x_j$ appears at the intersection of the ith row and the jth column (Fig. 1.1). A binary operation

Fig. 1.1



$*$ on E is associative if $(\forall x, y, z \in E)x * (y * z) = (x * y) * z$. A group is a set G on which there is defined an associative law of composition $*$ such that

(*a*) there is an identity element (i.e. an element e such that $(\forall x \in G)e * x = x = x * e$);

(*b*) every element of G has an inverse (i.e. for every $x \in G$ there exists $y \in G$ such that $x * y = e = y * x$).

When the law of composition is written as addition (respectively multiplication) we denote the identity element by 0 (respectively 1) and the inverse of $x \in G$ by $-x$ (respectively x^{-1}). Elements x, y of a group G are said to commute if $xy = yx$, and the group is said to be abelian if every pair of elements commute.

In studying algebraic structures there are two important notions to consider. The first is that of a substructure, and the other is that of a structure-preserving mapping from one such structure to another.

A subgroup of a group G is a non-empty subset H with the property that H is closed (or stable) under the operation of G (i.e. $x, y \in H \Rightarrow xy \in H$) and is also a group under the law of composition that is thus inherited from G. To show that a non-empty subset H is a subgroup of G it suffices to prove that H satisfies the property

$$x, y \in H \Rightarrow xy^{-1} \in H.$$

In additive notation, this becomes

$$x, y \in H \Rightarrow x - y \in H.$$

Alternatively, one can check that H is stable and that $y \in H \Rightarrow y^{-1} \in H$. In order to prove that a particular set H together with a given law of composition forms a group, it is often best to show that H is a subgroup of a larger set which is known to be a group. For example, the set $2\mathbb{Z}$ of even integers is a group under addition, being a subgroup of the additive group $\mathbb{Z}$. If G is a group and S is a non-empty subset of G then the smallest subgroup of G that contains S is denoted by $\langle S \rangle$ and consists of all products of powers of elements of S. In particular, if $S = \{g\}$ then the subgroup $\langle S \rangle = \langle g \rangle$ is said to be cyclic. It is given by:

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$$

where $g^0 = 1$. Note that all the powers of g need not be distinct : it is possible to have $g^m = g^n$ with $m \neq n$, so that $g^{m-n} = 1$. The smallest positive integer k (when it exists) such that $g^k = 1$ is called the order of g in G. When no such k exists, G is said to have infinite order. This should not be confused with what is called the order of the group G, namely the number $|G|$ of elements in G. Nevertheless, note that $|\langle g \rangle|$ is equal to the order of g. For every positive integer n there is a cyclic group of order n. This is denoted by C_n. All subgroups of C_n are of the form C_m where m divides n. The celebrated theorem of Lagrange states that for a finite group the order of every subgroup divides the order of the group; i.e. if H is a subgroup of G then $|H|$ is a factor of $|G|$.

The usual proof of Lagrange's theorem uses the notion of a coset. If H is a subgroup of G then the right cosets (respectively left cosets) of H in G are the sets $Hx = \{hx \mid h \in H\}$ (respectively $xH = \{xh \mid h \in H\}$). The set of right (respectively left) cosets of H in G forms a partition of G and the number of cosets is called the index of H in G. A subgroup H of G is said to be normal in G if $(\forall x \in G)xH = Hx$. When H is normal, the set of cosets forms a group under the law of composition given by $xH.yH = xyH$. This group is called the quotient group of G by H and is written G/H.

The notion of a normal subgroup is intimately related to that of a structure-preserving mapping. If G, H are groups then a mapping $f : G \to H$ is called a group morphism if $(\forall x, y \in G)f(xy) = f(x)f(y)$. Group morphisms are very often called homomorphisms. A bijective group morphism is called an isomorphism. There are two important subsets associated with every group morphism $f : G \to H$, namely the kernel and image of f, defined respectively by

$$\operatorname{Ker} f = \{x \in G \mid f(x) = 1\};$$
$$\operatorname{Im} f = \{f(x) \mid x \in G\}.$$

For every group morphism $f : G \to H$, $\operatorname{Ker} f$ is a normal subgroup of G. Conversely, every normal subgroup is the kernel of some group morphism. The first isomorphism theorem for groups states that if $f : G \to H$ is a group morphism then $\operatorname{Im} f$ is isomorphic to $G/\operatorname{Ker} f$; in symbols, $\operatorname{Im} f \cong G/\operatorname{Ker} f$.

We assume that the reader is familiar with the notion of a permutation (simply a bijection on a finite set) and the notation

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

as well as the cycle notation for permutations. Here we treat permutations precisely as mappings, so that multiplication of permutations is their composition as mappings. For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

or, in cycle notation,

$$(1\ 3)(1\ 2) = (1\ 2\ 3).$$

The set of all permutations on a set of n elements (which is usually chosen to be $\{1, 2, \dots, n\}$) is a multiplicative group denoted by S_n.

As an illustration of the first isomorphism theorem, consider the mapping $\vartheta : S_3 \to S_3$ defined by

$$\vartheta(x) = \begin{cases} (1) & \text{if } x \text{ is even;} \\ (1\ 2) & \text{if } x \text{ is odd.} \end{cases}$$

ϑ is a group morphism and $S_2 \cong \text{Im } \vartheta \cong S_3/\text{Ker } \vartheta$ where $\text{Ker } \vartheta = \{(1), (1\ 2\ 3), (3\ 2\ 1)\}$ is the cyclic subgroup of S_3 generated by $\{(1\ 2\ 3)\}$.

1.1 Show that the prescription

$$[a][b] = [ab]$$

defines a binary operation on the set $\mathbb{Z}_n$ of congruence classes modulo n. Show also that the prescription

$$[a] + [b] = [a + b]$$

defines a binary operation on $\mathbb{Z}_n$.

Find $[a], [b] \in \mathbb{Z}_6$ with $[a] \neq [0]$ so that the equation

$$[a][x] = [b]$$

has (a) no solution, (b) exactly one solution for $[x] \in \mathbb{Z}_6$. Is it possible to find $[a], [b] \in \mathbb{Z}_6$ so that the equation has more than one solution?

1.2 Let R be the equivalence relation defined on $\mathbb{Z}$ by

$$xRy \text{ if and only if } x^2 \equiv y^2 \pmod 6.$$

Let S denote the set of equivalence classes. Show that $[x]_R[y]_R = [xy]_R$ defines a binary operation on S and compile the associated Cayley table. Does $[x]_R + [y]_R = [x + y]_R$ define a binary operation on S?

1.3 Let $P = \{p \in \mathbb{Z} \mid p \text{ is a prime and } p \leqslant 13\}$. Define a binary operation $*$ on P by

$$p * q = \text{the greatest prime divisor of } p + q - 2.$$

Construct the Cayley table for $*$ and show that P has an identity with respect to $*$. Does every element of P have an inverse? Is $*$ associative?

1.4 A binary operation $*$ is defined on $E = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ by

$$(x, y, z) * (x', y', z') = (xx', \alpha y' + yx', \alpha z' + zx')$$

where $\alpha = x + y + z$. Show that $*$ is associative and that E contains an identity with respect to $*$. Show also that (x, y, z) has an inverse if and only if x and α are both non-zero. Find the inverse of (x, y, z) when it exists.

1.5 For each of the following sets, determine whether the given operation is associative. Does the set contain an identity for the given operation? If it has an identity does every element have an inverse? Is the set a group under the given operation?

(*a*) The even integers under addition.
(*b*) The rationals under subtraction.
(*c*) The rationals under multiplication.
(*d*) The positive rationals under multiplication.
(*e*) $\mathbb{Z}_6 \setminus \{[0]\}$ under multiplication.
(*f*) $\mathbb{Z}_5$ under multiplication.
(*g*) The cube roots of 1 under multiplication.

1.6 Which of the following sets are groups under the operation $*$ given?
(*a*) Positive integers with $a * b = \max\{a, b\}$.
(*b*) $\mathbb{Z}$ with $a * b = \min\{a, b\}$.
(*c*) $\mathbb{R}$ with $a * b = a + b - ab$.
(*d*) Positive integers with $a * b = \max\{a, b\} - \min\{a, b\}$.
(*e*) $\mathbb{Z} \times \mathbb{Z}$ with $(a, b) * (c, d) = (a + c, b + d)$.
(*f*) $\mathbb{R} \times \mathbb{R}$ with $(a, b) * (c, d) = (ac + bd, ad + bd)$.
(*g*) $(\mathbb{R} \times \mathbb{R}) \setminus \{(0, 0)\}$ with $(a, b) * (c, d) = (ac - bd, ad + bc)$.

1.7 Let T be the set of matrices of the form

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

where $x, y \in \mathbb{R}$. Prove that T is a group under matrix addition, and that $T \setminus \{0\}$ is a group under matrix multiplication.

1.8 Let G be the set of mappings $f : \mathbb{R} \to \mathbb{R}$ of the form $f(x) = ax + b$ with $a \neq 0$. Prove that G forms a group under composition of mappings.

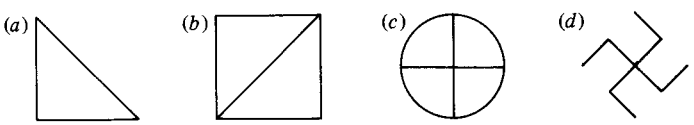
1.9 Define a binary operation $*$ on $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ by

$$a * b = \begin{cases} ab & \text{if } a > 0; \\ \dfrac{a}{b} & \text{if } a < 0. \end{cases}$$

Is $\mathbb{R}^*$ a group under $*$?

1.10 Determine the group of symmetries of each of the figures in Fig. 1.2.

Fig.1.2



1.11 Prove that the group of symmetries of a regular n-sided polygon (with $n \geqslant 3$) has $2n$ elements and describe them. Prove that none of these *dihedral groups* is abelian.

1.12 Consider the infinite pattern

$$\ldots \forall\forall\forall\forall\forall \ldots$$

Clearly the symmetries of this consist of

(a) translations a number of units in either direction;

(b) reflections in a vertical line either through the centre of any symbol or between two symbols.

Let a be the translation one unit to the right and let b be the reflection in a vertical line through the centre of a fixed symbol. Show that the group of symmetries is generated by a and b subject to the relations $b^2 = 1$, $ba = a^{-1}b$.

There are seven 'linear' patterns with different symmetry groups. Can you find them all?

1.13 Let G be the group of rotations of a cube. Show that $|G| = 24$. Find eight different non-identity elements satisfying $x^3 = 1$ which fix a corner. Find nine non-identity elements satisfying $x^4 = 1$ which take a given face to itself. Find six non-identity elements satisfying $x^2 = 1$ which take a given edge to itself. Check that each of the 24 elements has now been identified.

Do the same for the group of rotations of an octahedron (the regular solid with six vertices and eight triangular faces).

(*Hint*: This can be deduced easily from the group of rotations of a cube!)

1.14 The following is part of the Cayley table of a finite group. Fill in the missing entries:

	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	y		
b	b					
x	x	z				a
y	y					
z	z					

1.15 Use Lagrange's theorem to show that if G is a group with $|G| = n$ then $g^n = 1$ for every $g \in G$. Deduce that if p is a prime then $a^p \equiv a \pmod{p}$ for any

integer a. Hence find the remainder on dividing

(a) 7^{100} by 11;

(b) 9^{37} by 13.

1.16 Let G be a group and let $a, b \in G$ be such that $ab = ba^k$ where k is a fixed positive integer. Prove by induction that, for all positive integers n,

(a) $a^n b = ba^{kn}$;

(b) $ab^n = b^n a^{k^n}$.

Suppose now that b is of order 2. Prove that $(ba^n)^2$ commutes with both a and b.

1.17 Let G be a group and let $a, b \in G$ be such that $ab \neq ba$. Prove that the elements $1, a, b, ab, ba$ are distinct. Show further that either $a^2 = 1$ or $a^2 \notin \{1, a, b, ab, ba\}$. In the case where $a^2 = 1$ show that $aba \notin \{1, a, b, ab, ba\}$. Deduce that every non-abelian group contains at least six elements.

Let F be the set of six functions from $\mathbb{R} \setminus \{0, 1\}$ to itself given by

$$e(x) = x, \quad p(x) = \frac{1}{1-x}, \quad q(x) = \frac{x-1}{x},$$

$$a(x) = \frac{1}{x}, \quad b(x) = 1-x, \quad c(x) = \frac{x}{x-1}.$$

Construct the Cayley table for F under $\circ$ and show that F is a non-abelian group.

1.18 (a) Let a and b be elements of a group G which commute. Prove that a and b^{-1} commute. Prove also that if x is any element of G then xax^{-1} and xbx^{-1} commute.

(b) Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

(c) Prove that if G is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$ then G is abelian.

(d) Let G be a group and suppose that $a^2 = 1$ for every $a \in G$. Prove that G is abelian.

(e) If G is a group and $x, y \in G$ prove by induction that, for every positive integer n, $(x^{-1}yx)^n = x^{-1}y^n x$.

(f) Let G be a group and suppose that $a, b \in G$ are such that $b^6 = 1$ and $ab = b^4a$. Prove that $b^3 = 1$ and that $ab = ba$.

1.19 Let G be the multiplicative group of non-singular 2×2 matrices with rational entries. What are the orders of the following elements of G?

$$\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ -\frac{3}{2} & -\frac{1}{2} \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Find an element of order 2 in G.

Prove by induction that if

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ then } A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

for every $n \in \mathbb{N}$. Deduce that A does not have finite order. Is G a finite group? Find $a, b, c \in G$ such that a and b commute, b and c commute but a and c do not commute.

1.20 Which of the following groups are abelian? Which are cyclic? Which are finite?

(*a*) $G = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}$ under multiplication.

(*b*) The non-zero elements of $\mathbb{Z}_{11}$ under multiplication.

(*c*) The group of bijections of $E = \{1, 2, 3\}$ to itself under composition of mappings.

(*d*) The group of bijections of $E = \{1, 2\}$ to itself under composition of mappings.

(*e*) The even integers under addition.

(*f*) $\mathbb{R}$ under addition.

1.21 On the set $G = \mathbb{R} \setminus \{0\} \times \mathbb{R}$ define a law of composition by

$$(a, b)(c, d) = (ac, bc + d).$$

Prove that G is a non-abelian group.

Determine which of the following subsets of G are subgroups.

$H = \{(a, k(a-1)) \mid a \neq 0\}$ where $k \in \mathbb{R}$ is fixed;

$K = \{(a, 0) \mid a > 0\}$;

$L = \{(a, na^n) \mid a \neq 0\}$ where $n \in \mathbb{N}$ is fixed;

$M = \{(1, b) \mid b \in \mathbb{R}\}$.

Show that G contains an infinite number of elements of order 2. Does G contain elements of order 3?

1.22 (*a*) Let G denote the group of non-zero rationals under multiplication. Let

$$H = \{2^n \mid n \in \mathbb{Z}\}, \quad K = \left\{ \frac{1 + 2n}{1 + 2m} \mid n, m \in \mathbb{Z} \right\}.$$

Are H and K subgroups of G?

(*b*) Show that $H = \{[0], [4], [8], [12]\}$ is a subgroup of $\mathbb{Z}_{16}$ under addition.

(*c*) Find all the subgroups of the group in question 1.14.

1.23 Let $S = \{(x, y) \mid x, y \in \mathbb{R}, x \neq 0, x + y \neq 0\}$. Prove that the binary operation defined on S by

$$(x_1, y_1)(x_2, y_2) = (x_1x_2, (x_1 + y_1)(x_2 + y_2) - x_1x_2)$$

makes S into a group.

Show that $P = \{(1, y) \mid y > -1\}$ is a subgroup of S.

1.24 Prove that

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

is a group under multiplication. Let H_N be the subset of G consisting of those matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in G with

$$a \equiv d \equiv 1 (\text{mod } N), \quad b \equiv c \equiv 0 (\text{mod } N),$$

N being a fixed positive integer. Prove that H_N is a subgroup of G.

If $S = \{H_N \mid 2 \leqslant N \leqslant 12\}$ is ordered by a set inclusion, draw the Hasse diagram for S.

1.25 Let p be an odd prime. A non-zero integer a is said to be a *quadratic residue* of p if there exists an integer x such that $x^2 \equiv a (\text{mod } p)$. Prove that

(*a*) the quadratic residues of p form a subgroup Q of the group of non-zero integers mod p under multiplication;

(*b*) $|Q| = \frac{1}{2}(p - 1)$;

(*c*) if $q \in Q, n \notin Q$ then nq is not a quadratic residue;

(*d*) if m and n are not quadratic residues then mn is a quadratic residue;

(*e*) if a is a quadratic residue then $a^{(p-1)/2} \equiv 1 (\text{mod } p)$.

1.26 Let $M = \{M(\vartheta) \mid \vartheta \in \mathbb{R}\}$ where

$$M(\vartheta) = \begin{bmatrix} \cos \vartheta & -\sin \vartheta \\ \sin \vartheta & \cos \vartheta \end{bmatrix}.$$

Prove that M is an abelian group. Show that M contains cyclic subgroups of every finite order. Does M contain infinite cyclic subgroups?

1.27 Let $G = \langle g \rangle$ be a cyclic group of finite order n generated by the element

g. What are the subgroups of G? Prove that the other generators of G are the elements g^r where hcf $\{r, n\} = 1$.

For the group $\mathbb{Z}_{18}$ list all the subgroups and find all the generators in each subgroup. Draw the subgroup Hasse diagram.

1.28 Prove that if G is a group and H, K are subgroups of G then $H \cap K$ is a subgroup of G. Suppose now that G is finite and that hcf $\{|H|, |K|\} = 1$. Prove that $H \cap K = \{1\}$.

Find $m\mathbb{Z} \cap n\mathbb{Z}$ in the additive group $\mathbb{Z}$. Deduce that no two non-trivial subgroups of $\mathbb{Z}$ can intersect in the trivial subgroup.

1.29 Suppose that G is a group. For every $a \in G$ define

$$C(a) = \{x \in G \mid ax = xa\}.$$

Prove that $C(a)$ is a subgroup of G.

Now suppose that H is a subgroup of G. Define

$$C(H) = \{x \in G \mid (\forall a \in H)ax = xa\}.$$

Prove that $C(H)$ is a subgroup of G.

Give examples of situations where

(*a*) $C(H) = H$;
(*b*) $C(H) = \{1\}$;
(*c*) $H \neq G$ and $C(H) = G$.

1.30 If G is an abelian group and $a, b \in G$ are distinct elements of order 2, show that ab has order 2. Prove that $\{1, a, b, ab\}$ forms a subgroup of G that is not cyclic.

Consider the set

$$G = \{[n] \mid n \text{ an odd integer}\},$$

where $[n]$ denotes the congruence class of n modulo 2^{k+1} and k is a fixed integer greater than 1. Given that G is a group under the usual multiplication of congruence classes show, by considering the elements $[2^k - 1]$ and $[2^k + 1]$, that G is not cyclic.

1.31 Let $\mathbb{Q}$ be the additive group of rationals. If

$$r_1 = \frac{p_1}{q_1} \in \mathbb{Q} \text{ and } r_2 = \frac{p_2}{q_2} \in \mathbb{Q}$$

prove that

$$\langle r_1, r_2 \rangle \subseteq \left\langle \frac{1}{q_1 q_2} \right\rangle .$$