Mathematics Course 111: Algebra I
Part II: Groups

D. R. Wilkins

Academic Year 1996-7

6 Groups

A *binary operation* $*$ on a set G associates to elements x and y of G a third element $x * y$ of G. For example, addition and multiplication are binary operations of the set of all integers.

Definition. A *group* G consists of a set G together with a binary operation $*$ for which the following properties are satisfied:

- $(x * y) * z = x * (y * z)$ for all elements x, y, and z of G (the *Associative Law*);
- there exists an element e of G (known as the *identity element* of G) such that $e * x = x = x * e$, for all elements x of G;
- for each element x of G there exists an element x' of G (known as the *inverse* of x) such that $x * x' = e = x' * x$ (where e is the identity element of G).

The *order* $|G|$ of a finite group G is the number of elements of G.

A group G is *Abelian* (or *commutative*) if $x * y = y * x$ for all elements x and y of G.

One usually adopts *multiplicative notation* for groups, where the product $x * y$ of two elements x and y of a group G is denoted by xy. The inverse of an element x of G is then denoted by x^{-1}. The identity element is usually denoted by e (or by e_G when it is necessary to specify explicitly the group to which it belongs). Sometimes the identity element is denoted by 1. Thus, when multiplicative notation is adopted, the group axioms are written as follows:-

- $(xy)z = x(yz)$ for all elements x, y, and z of G (the *Associative Law*);
- there exists an element e of G (known as the *identity element* of G) such that $ex = x = xe$, for all elements x of G;
- for each element x of G there exists an element x^{-1} of G (known as the *inverse* of x) such that $xx^{-1} = e = x^{-1}x$ (where e is the identity element of G).

The group G is said to be *Abelian* (or *commutative*) if $xy = yx$ for all elements x and y of G.

It is sometimes convenient or customary to use additive notation for certain groups. Here the group operation is denoted by $+$, the identity element of the group is denoted by 0, the inverse of an element x of the group is denoted by $-x$. By convention, additive notation is only used for Abelian groups. When expressed in additive notation the axioms for a Abelian group are as follows:

- $x + y = y + x$ for all elements x and y of G (the *Commutative Law*);

- $(x + y) + z = x + (y + z)$ for all elements x, y, and z of G (the *Associative Law*);
- there exists an element 0 of G (known as the *identity element* or *zero element* of G) such that $0 + x = x = x + 0$, for all elements x of G;
- for each element x of G there exists an element $-x$ of G (known as the *inverse* of x) such that $x + (-x) = 0 = (-x) + x$ (where 0 is the identity element of G).

We shall usually employ multiplicative notation when discussing general properties of groups. Additive notation will be employed for certain groups (such as the set of integers with the operation of addition) where this notation is the natural one to use.

Examples of groups

Example. The set of all integers is an Abelian (or commutative) group under the operation of addition. (Additive notation is of course normally employed for this group.)

Example. The set of all rational numbers is an Abelian group under the operation of addition. (Additive notation is of course normally employed for this group.)

Example. The set of all real numbers is an Abelian group under the operation of addition. (Additive notation is of course normally employed for this group.)

Example. The set of all complex numbers is an Abelian group under the operation of addition. (Additive notation is of course normally employed for this group.)

Example. The set of all 2×2 matrices is an Abelian group under the operation of addition. (Additive notation is of course normally employed for this group.)

Example. The set of all (2-dimensional) vectors is an Abelian group under the operation of addition. (Addition of vectors is defined through the 'Parallelogram Law'. Additive notation is of course normally employed for this group.)

Example. The set of all non-zero rational numbers is an Abelian group under the operation of multiplication.

Example. The set of all non-zero real numbers is an Abelian group under the operation of multiplication.

Example. The set of all non-zero complex numbers is an Abelian group under the operation of multiplication.

Example. The set of all non-zero complex numbers is an Abelian group under the operation of multiplication.

Example. Let n be a positive integer. The set $\mathbb{Z}_n$ of congruence classes of integers modulo n is a group with respect to the operation of addition. (Additive notation is of course normally employed for this group.)

Example. It can be shown that the set $\mathbb{Z}_n^*$ of non-zero congruence classes modulo n is a group with respect to the operation of multiplication if and only if n is a prime number.

Example. The set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with real (or complex) entries satisfying $ad - bc \neq 0$ is a group under the operation of matrix multiplication. This group is not Abelian.

Example. The set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with real (or complex) entries satisfying $ad - bc = 1$ is a group under the operation of matrix multiplication. This group is not Abelian.

Example. The set of all transformations of the plane that are of the form

$$(x, y) \mapsto (ax + by, cx + dy)$$

with $ad - bc \neq 0$ is a group with respect to the operation of composition of transformations. This group includes all rotations about the origin, and all reflections in lines passing through the origin. It is not Abelian.

Example. Consider a regular n-sided polygon centered at the origin. The symmetries of this polygon (i.e., length- and angle-preserving transformations of the plane that map this polygon onto itself) are rotations about the origin through an integer multiple of $2\pi/n$ radians, and reflections in the n axes of symmetry of the polygon. The symmetries of the polygon constitute a group of order $2n$. This group is referred to as the *dihedral group of order* $2n$.

Example. The symmetries of a rectangle that is not a square constitute a group of order 4. This group consists of the identity transformation, reflection in the axis of symmetry joining the midpoints of the two shorter sides, reflection in the axis of symmetry joining the two longer sides, and rotation though an angle of π radians (180°). If I denotes the identity transformation, A and B denote the reflections in the two axes of symmetry, and C denotes the rotation through π radians then $A^2 = B^2 = C^2 = I$, $AB = BA = C$, $AC = CA = B$ and $BC = CB = A$. This group is Abelian: it is often referred to as the *Klein 4-group* (or, in German, *Kleinsche Viergruppe*).

Example. The group of symmetries of a regular tetrahedron in 3-dimensional space constitute a group. Any permutation of the vertices of the tetrahedron can be effected by an appropriate symmetry of the tetrahedron. Moreover each symmetry is completely determined by the permutation of the vertices which it induces. Therefore the group of symmetries of a regular tetrahedron is of order 24, since there are 24 permutations of a set with four elements. It turns out that this group is non-Abelian.

Example. The set of all permutations of a set is a group with respect to the operation of composition. For each positive integer n the group of all permutations of the set $\{1, 2, \ldots, n\}$ is a group of order $n!$, referred to as the *symmetric group on n letters*, and is usually denoted by S_n (or by Σ_n).

Example. The set of all *even* permutations of a finite set is a group with respect to the operation of composition. For each integer n greater than one, the group of all even permutations of the set $\{1, 2, \ldots, n\}$ is a group of order $n!/2$, referred to as the *alternating group on n letters*, and is usually denoted by A_n.

Cayley Tables

The algebraic structure of a finite group can be exhibited using a *Cayley table*, provided that the number of elements in the group is sufficiently small. The rows and columns of the Cayley table are labelled by the elements of the group, and each entry in the table is the product xy of the element x labelling its row with the element y labelling its column.

Example. Let D_6 be the group of symmetries of an equilateral triangle with vertices labelled A, B and C in anticlockwise order. The elements of D_6 consist of the identity transformation $\mathbf{I}$, an anticlockwise rotation $\mathbf{R}$ about the centre through an angle of $2\pi/3$ radians (i.e., 120°), a clockwise rotation $\mathbf{S}$ about the centre through an angle of $2\pi/3$ radians, and reflections $\mathbf{U}$, $\mathbf{V}$ and $\mathbf{W}$ in the lines joining the vertices A, B and C respectively to the midpoints of the opposite edges. Calculating the compositions of these rotations, we obtain the following Cayley table:

	I	**R**	**S**	**U**	**V**	**W**
I	**I**	**R**	**S**	**U**	**V**	**W**
R	**R**	**S**	**I**	**W**	**U**	**V**
S	**S**	**I**	**R**	**V**	**W**	**U**
U	**U**	**V**	**W**	**I**	**R**	**S**
V	**V**	**W**	**U**	**S**	**I**	**R**
W	**W**	**U**	**V**	**R**	**S**	**I** .

Thus, for example, $\mathbf{VU} = \mathbf{S}$ (i.e., the reflection $\mathbf{U}$ followed by the reflection $\mathbf{V}$ is the rotation $\mathbf{S}$), and $\mathbf{UV} = \mathbf{R}$.

Note that each element of the group occurs exactly once in each row and in each column in the main body of the table (excluding the labels at the left of each row and at the head of each column), This is a general property of Cayley tables of groups which can be proved easily from the group axioms.

Elementary Properties of Groups

In what follows, we describe basic properties of a group G, using multiplicative notation and denoting the identity element of the group by the letter e.

Lemma 6.1. *A group G has exactly one identity element e satisfying $ex = x = xe$ for all $x \in G$.*

Proof. Suppose that f is an element of G with the property that $fx = x$ for all elements x of G. Then in particular $f = fe = e$. Similarly one can show that e is the only element of G satisfying $xe = x$ for all elements x of G. ▮

Lemma 6.2. *An element x of a group G has exactly one inverse x^{-1}.*

Proof. We know from the axioms that the group G contains at least one element x^{-1} which satisfies $xx^{-1} = e$ and $x^{-1}x = e$. If z is any element of G which satisfies $xz = e$ then $z = ez = (x^{-1}x)z = x^{-1}(xz) = x^{-1}e = x^{-1}$. Similarly if w is any element of G which satisfies $wx = e$ then $w = x^{-1}$. In particular we conclude that the inverse x^{-1} of x is uniquely determined, as required. ▮

Lemma 6.3. *Let x and y be elements of a group G. Then $(xy)^{-1} = y^{-1}x^{-1}$.*

Proof. It follows from the group axioms that

$$(xy)(y^{-1}x^{-1}) = x(y(y^{-1}x^{-1})) = x((yy^{-1})x^{-1}) = x(ex^{-1}) = xx^{-1} = e.$$

Similarly $(y^{-1}x^{-1})(xy) = e$, and thus $y^{-1}x^{-1}$ is the inverse of xy, as required. ▮

Note in particular that $(x^{-1})^{-1} = x$ for all elements x of a group G, since x has the properties that characterize the inverse of the inverse x^{-1} of x.

Given an element x of a group G, we define x^n for each positive integer n by the requirement that $x^1 = x$ and $x^n = x^{n-1}x$ for all $n > 1$. (This is an example of a so-called *inductive definition*, where some quantity $u(n)$ is defined for all positive integers n by specifying $u(1)$ and also the rule that determines $u(n)$ in terms of $u(n-1)$ for each $n > 1$.) We also define $x^0 = e$, where e is the identity element of the group, and we define x^{-n} to be the inverse of x^n for all positive integers n.

Theorem 6.4. *Let x be an element of a group G. Then $x^{m+n} = x^m x^n$ and $x^{mn} = (x^m)^n$ for all integers m and n.*

Proof. The relevant definitions ensure that $x^{m+n} = x^m x^n$ whenever $m \geq 0$ and $n = 0$ or 1. Suppose that $x^{m+k} = x^m x^k$ for some positive integer k. Then

$$x^{m+k+1} = x^{m+k}x = (x^m x^k)x = x^m(x^k x) = x^m x^{k+1}.$$

It therefore follows by induction on n that $x^{m+n} = x^m x^n$ for non-negative integers m and n.

Let p and q be non-negative integers. Then

$$x^{-p-q} = (x^{p+q})^{-1} = (x^q x^p)^{-1} = (x^p)^{-1}(x^q)^{-1} = x^{-p}x^{-q}$$

We deduce from this that $x^{m+n} = x^m x^n$ when m and n are both negative.

Now let p and q be non-negative integers with $p \leq q$. Then $x^q = x^p x^{q-p}$ and $x^q = x^{q-p}x^p$. On multiplying these identities by x^{-p} on the left and right respectively, we deduce that $x^{q-p} = x^q x^{-p}$ and $x^{q-p} = x^{-p}x^q$. On taking inverses, we see also that $x^{p-q} = x^p x^{-q}$ and $x^{p-q} = x^{-q}x^p$. We can apply these formulae either with $p = |m|$ and $q = |n|$ (in the case when $|m| \leq |n|$), or with $p = |n|$ and $q = |m|$ (in the case when $|m| \geq |n|$), to deduce that $x^{m+n} = x^m x^n$ whenever m and n have opposite signs. Combining this result with the corresponding results when m and n have the same sign, we deduce that $x^{m+n} = x^m x^n$ for all integers m and n.

The identity $x^{mn} = (x^m)^n$ follows immediately from the definitions when $n = 0$, 1 or -1. If $x^{mk} = (x^m)^k$ for some integer k then $x^{m(k+1)} = x^{mk+m} = x^{mk}x^m = (x^m)^k x^m = (x^m)^{k+1}$. It follows by induction on n that $x^{mn} = (x^m)^n$ for all positive integers n. The result when n is a negative integer then follows on taking inverses. Thus $x^{mn} = (x^m)^n$ for all integers m and n, as required. ▮

If additive notation is employed for an Abelian group then the notation 'x^n' is replaced by 'nx' for all integers n and elements x of the group. The analogue of Theorem 6.4 then states that $(m+n)x = mx + nx$ and $(mn)x = m(n(x))$ for all integers m and n.

The General Associative Law

Let $x_1, x_2, \ldots, x_n$ be elements of a group G. We define the product $x_1 x_2 \cdots x_n$ as follows:-

$$\begin{aligned} x_1x_2x_3 &= (x_1x_2)x_3 \\ x_1x_2x_3x_4 &= (x_1x_2x_3)x_4 = ((x_1x_2)x_3)x_4 \\ x_1x_2x_3x_4x_5 &= (x_1x_2x_3x_4)x_5 = (((x_1x_2)x_3)x_4)x_5 \\ &\vdots \\ x_1x_2x_3\cdots x_n &= (x_1x_2\cdots x_{n-1})x_n = (\cdots((x_1x_2)x_3)\cdots x_{n-1})x_n. \end{aligned}$$

(Thus if $p_j = x_1, x_2, \ldots, x_j$ for $j = 1, 2, \ldots, n$ then $p_j = p_{j-1}x_j$ for each $j > 1$.)

Now an arbitrary product of n elements of G is determined by an expression involving n elements of G together with equal numbers of left and right parentheses that determine the order in which the product is evaluated. The *General Associative Law* ensures that the value of such a product is determined only by the order in which the elements of the group occur within that product. Thus a product of n elements of G has the value $x_1x_2\cdots x_n$, where $x_1, x_2, \ldots, x_n$ are the elements to be multiplied, listed in the order in which they occur in the expression defining the product.

Example. Given four elements x_1, x_2, x_3 and x_4 of a group, the products

$$((x_1x_2)x_3)x_4, \quad (x_1x_2)(x_3x_4), \quad (x_1(x_2x_3))x_4, \quad x_1((x_2x_3)x_4), \quad x_1(x_2(x_3x_4))$$

all have the same value. (Note that $x_1x_2x_3x_4$ is by definition the value of the first of these expressions.)

The General Associative Law for products of four or more elements of a group can be verified by induction on the number on the number of elements involved.

Consider a product of n elements of the group G, where $n > 3$. Let these elements be $x_1, x_2, \ldots, x_n$ when listed in the order in which they occur in the expression for the product. Suppose also that it is known that the General Associative Law holds for all products involving fewer than n elements (i.e., any two products with fewer than n elements have the same value whenever the same elements of G occur in both products in the same order). We must show that the value of the product is $x_1x_2\cdots x_n$, where

$$x_1x_2\cdots x_n = (\ldots(((x_1x_2)x_3)x_4)\cdots)x_n$$

Now the first step in evaluating the product will involve multiplying some element x_r with the succeeding element x_{r+1}. The subsequent steps will then evaluate a product of $n-1$ elements, namely the elements x_i for $1 \leq i < r$, the element x_rx_{r+1}, and the elements x_i for $r + 1 < i \leq n$. The validity of the General Associative Law for products of fewer than n elements then ensures that the value p of the product is given by

$$p = \begin{cases} (x_1x_2)x_3\cdots x_n & \text{if } r = 1; \\ x_1(x_2x_3)x_4\cdots x_n & \text{if } r = 2; \\ x_1x_2(x_3x_4)x_5\cdots x_n & \text{if } r = 3 \text{ (and } n > 4); \\ \vdots & \\ x_1x_2\cdots x_{n-2}(x_{n-1}x_n) & \text{if } r = n-1. \end{cases}$$

Also the General Associativity Law for products of fewer than n elements ensures that if $r < n - 1$ then

$$x_1x_2\cdots x_{r-1}(x_rx_{r+1}) = x_1x_2\cdots x_{r+1}$$

and thus $p = x_1x_2\cdots x_n$. Thus in order to verify the General Associative Law for products of n elements it only remains to verify that

$$x_1x_2\cdots x_{n-2}(x_{n-1}x_n) = x_1x_2\cdots x_n.$$

The case when $n = 3$ is the Associative Law for products of three elements. For $n > 3$ let y be the product $x_1x_2, \cdots x_{n-2}$ of the elements $x_1, x_2, \ldots, x_{n-2}$ (with $y = x_1x_2$ in the case when $n = 4$). Then

$$\begin{aligned} x_1x_2\cdots x_{n-2}(x_{n-1}x_n) &= y(x_{n-1}x_n) = (yx_{n-1})x_n = (x_1x_2\cdots x_{n-1})x_n \\ &= x_1x_2\cdots x_n. \end{aligned}$$

We have thus shown that if the General Associative Law holds for all products involving fewer than n elements of the group G, then it holds for all products involving n elements of G. The validity of the General Associative Law therefore follows by induction on the number of elements occurring in the product in question.

Note that the only group axiom used in verifying the General Associative Law is the Associative Law for products of three elements. It follows from this that the General Associative Law holds for any binary operation on a set that satisfies the Associative Law for products of three elements. (A set with a binary operation satisfying the Associative Law is referred to as a *semigroup*—the General Associative Law holds in all semigroups.)

Subgroups

Definition. Let G be a group, and let H be a subset of G. We say that H is a *subgroup* of G if the following conditions are satisfied:

- the identity element of G is an element of H;
- the product of any two elements of H is itself an element of H;
- the inverse of any element of H is itself an element of H.

Example. The group of integers is a subgroup of the groups of rational numbers, real numbers and complex numbers under addition.

Example. The group of non-zero rational numbers is a subgroup of the groups of non-zero real numbers and non-zero complex numbers under multiplication.

Example. The group of all 2×2 matrices of real numbers with determinant equal to 1 is a subgroup of the group of all 2×2 matrices of real numbers with non-zero determinant under the operation of matrix multiplication.

Example. Consider the collection of all 2×2 matrices that are of the form $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ for some real number α. This is a subgroup of the group of all 2×2 matrices with non-zero determinant under matrix multiplication. Indeed the above matrix is the identity matrix when $\alpha = 0$. Also

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} = \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix}$$

(as can be seen from the well-known formulae giving $\sin(\alpha+\beta)$ and $\cos(\alpha+\beta)$ in terms of α and β), and

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}^{-1} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix}$$

for all real numbers α and β. Thus the definition of a subgroup is satisfied.

The corresponding geometrical result states that the set of all rotations of the plane about the origin is a subgroup of the group of all linear transformations of the plane that send a point (x, y) to $(ax + by, cx + dy)$ for some real numbers a, b, c and d satisfying $ad - bc \neq 0$.

Example. The group consisting of the identity permutation and the 3-cycles $(a\,b\,c)$ and $(a\,c\,b)$ is a subgroup of the group of all permutations of a set $\{a, b, c\}$ with three elements.

Example. The group consisting of the identity permutation and the permutations $(a\,b)\circ(c\,d)$, $(a\,c)\circ(b\,d)$ and $(a\,d)\circ(b\,c)$ is a subgroup of the group of all permutations of a set $\{a,b,c,d\}$ with four elements.

Example. The group of all rotations about the origin through some integer multiple of $2\pi/n$ radians is a subgroup of the dihedral group consisting of all symmetries of a regular n-sided polygon centred at the origin.

Example. Let g be an element of a group G, and let $C(g) = \{x \in G : xg = gx\}$. The identity element e of G belongs to $C(g)$, since the group axioms ensure that $eg = g = ge$. If x and y are elements of $C(g)$ then

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

and therefore xy is an element of $C(g)$. Also x^{-1} is an element of $C(g)$ for all elements x of $C(g)$, since $x^{-1}g = x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1} = gx^{-1}$. We conclude that $C(g)$ is a subgroup of the group G. The subgroup $C(g)$ is referred to as the *centralizer* of g.

Example. Let G be a group, and let $Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}$. Note that an element x of G belongs to $Z(G)$ if and only if it belongs to the centralizer $C(g)$ of each element g of G. It follows easily from this that $Z(G)$ is a subgroup of G. This subgroup is referred to as the *centre* of the group G.

Lemma 6.5. *Let g be an element of a group G. Then the set of all elements of G that are of the form g^n for some integer n is a subgroup of G.*

Proof. Let $H = \{g^n : n \in \mathbb{Z}\}$. Then the identity element belongs to H, since it is equal to g^0. The product of two elements of H is itself an element of H, since $g^m g^n = g^{m+n}$ for all integers m and n (see Theorem 6.4). Also the inverse of an element of H is itself an element of H since $(g^n)^{-1} = g^{-n}$ for all integers n. Thus H is a subgroup of G, as required. ▮

Definition. Let g be an element of a group G. The *order* of g is the smallest positive integer n for which $g^n = e$. The subgroup *generated* by g is the subgroup consisting of all elements of G that are of the form g^n for some integer n.

Lemma 6.6. *Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.*

Proof. The identity element of G belongs to $H \cap K$ since it belongs to the subgroups H and K. If x and y are elements of $H \cap K$ then xy is an element of H (since x and y are elements of H), and xy is an element of K, and therefore xy is an element of $H \cap K$. Also the inverse x^{-1} of an element x of $H \cap K$ belongs to H and to K and thus belongs to $H \cap K$, as required. ▮

More generally, the intersection of any collection of subgroups of a given group is itself a subgroup of that group.

Cyclic Groups

Definition. A group G is said to be *cyclic*, with generator g, if every element of G is of the form g^n for some integer n.

Example. The group $\mathbb{Z}$ of integers under addition is a cyclic group, generated by 1.

Example. Let n be a positive integer. The set $\mathbb{Z}_n$ of congruence classes of integers modulo n is a cyclic group of order n with respect to the operation of addition.

Example. The group of all rotations of the plane about the origin through an integer multiple of $2\pi/n$ radians is a cyclic group of order n for all integers n. This group is generated by an anticlockwise rotation through an angle of $2\pi/n$ radians.

Lemma 6.7. *Let G be a finite cyclic group with generator g, and let j and k be integers. Then $g^j = g^k$ if and only if $j - k$ is divisible by the order of the group.*

Proof. First we show that $g^m = e$ for some strictly positive integer m, where e is the identity element of G. Now $g^j = g^k$ for some integers j and k with $j < k$, since G is finite. Let $m = k - j$. Then $m > 0$ and $g^m = g^k(g^j)^{-1} = e$.

Let n be the smallest strictly positive integer for which $g^n = e$. Now any integer i can be expressed in the form $i = qn + r$, where q and r are integers and $0 \leq r < n$. (Thus q is the greatest integer for which $qn \leq i$.) Then $g^i = (g^n)^q g^r = g^r$ (since $g^n = e$). Now the choice of n ensures that $g^r \neq e$ if $0 < r < n$. It follows that an integer i satisfies $g^i = e$ if and only if n divides i.

Let j and k be integers. Now $g^j = g^k$ if and only if $g^{j-k} = e$, since $g^{j-k} = g^j(g^k)^{-1}$. It follows that $g^j = g^k$ if and only if $j - k$ is divisible by n. Moreover n is the order of the group G, since each element of G is equal to one of the elements g^i with $0 \leq i < n$ and these elements are distinct. ∎

We now classify all subgroups of a cyclic group G. Let g be a generator of G. Given a subgroup H of G with more than one element, let m be the smallest strictly positive integer for which $g^m \in H$. Suppose that $g^i \in H$ for some integer i. Now i can be expressed in the form $i = qm + r$, where q and r are integers and $0 \leq r < m$. (Thus q is the greatest integer for which $qm \leq i$.) But then $g^r = g^{i-qm} = g^i(g^m)^{-q}$, where $g^i \in H$ and $g^m \in H$, and therefore $g^r \in H$. The choice of m now ensures that $r = 0$, and hence $i = qm$. Thus $g^i \in H$ if and only if i is some integer multiple of m. This shows that H is the cyclic group generated by g^m, where m is the smallest strictly positive integer for which $g^m \in H$.

Let us consider the case when the cyclic group G is finite. Let s be the order of G. Then $g^s = e$, and hence g^s belongs to the subgroup H. It follows that s must be some integer multiple of m, where m is the smallest strictly positive integer for which $g^m \in H$. Thus the subgroups of a finite cyclic group G with generator g are the trivial subgroup $\{e\}$ and the cyclic subgroups generated by g^m for each divisor m of the order of G.

Consider now the case when the cyclic group G is infinite. For each positive integer m, the element g^m generates a subgroup of G, and moreover m is the smallest strictly positive integer for which g^m belongs to that subgroup. Thus if G is an infinite cyclic group with generator g then the subgroups of G are the trivial subgroup $\{e\}$ and the cyclic subgroups generated by g^m for each positive integer m.

We have thus classified all subgroups of a cyclic group. In particular we see that any subgroup of a cyclic group is itself a cyclic group.

Cosets and Lagrange's Theorem

Definition. Let H be a subgroup of a group G. A *left coset* of H in G is a subset of G that is of the form xH, where $x \in G$ and

$$xH = \{y \in G : y = xh \text{ for some } h \in H\}.$$

Similarly a *right coset* of H in G is a subset of G that is of the form Hx, where $x \in G$ and

$$Hx = \{y \in G : y = hx \text{ for some } h \in H\}.$$

Note that a subgroup H of a group G is itself a left coset of H in G.

Lemma 6.8. *Let H be a subgroup of a group G. Then the left cosets of H in G have the following properties:—*

(i) *$x \in xH$ for all $x \in G$;*

(ii) *if x and y are elements of G, and if $y = xa$ for some $a \in H$, then $xH = yH$;*

(iii) *if x and y are elements of G, and if $xH \cap yH$ is non-empty then $xH = yH$.*

Proof. Let $x \in G$. Then $x = xe$, where e is the identity element of G. But $e \in H$. It follows that $x \in xH$. This proves (i).

Let x and y be elements of G, where $y = xa$ for some $a \in H$. Then $yh = x(ah)$ and $xh = y(a^{-1}h)$ for all $h \in H$. Moreover $ah \in H$ and $a^{-1}h \in H$ for all $h \in H$, since H is a subgroup of G. It follows that $yH \subset xH$ and $xH \subset yH$, and hence $xH = yH$. This proves (ii).

Finally suppose that $xH \cap yH$ is non-empty for some elements x and y of G. Let z be an element of $xH \cap yH$. Then $z = xa$ for some $a \in H$, and $z = yb$ for some $b \in H$. It follows from (ii) that $zH = xH$ and $zH = yH$. Therefore $xH = yH$. This proves (iii). ∎

Lemma 6.9. *Let H be a finite subgroup of a group G. Then each left coset of H in G has the same number of elements as H.*

Proof. Let $H = \{h_1, h_2, \ldots, h_m\}$, where $h_1, h_2, \ldots, h_m$ are distinct, and let x be an element of G. Then the left coset xH consists of the elements xh_j for $j = 1, 2, \ldots, m$. Suppose that j and k are integers between 1 and m for which $xh_j = xh_k$. Then $h_j = x^{-1}(xh_j) = x^{-1}(xh_k) = h_k$, and thus $j = k$, since $h_1, h_2, \ldots, h_m$ are distinct. It follows that the elements $xh_1, xh_2, \ldots, xh_m$ are distinct. We conclude that the subgroup H and the left coset xH both have m elements, as required. ∎

Theorem 6.10. (Lagrange's Theorem) *Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.*

Proof. Each element of G belongs to at least one left coset of H in G, and no element can belong to two distinct left cosets of H in G (see Lemma 6.8). Therefore every element of G belongs to exactly one left coset of H. Moreover each left coset of H contains $|H|$ elements (Lemma 6.9). Therefore $|G| = n|H|$, where n is the number of left cosets of H in G. The result follows. ∎

Definition. Let H be a subgroup of a group G. If the number of left cosets of H in G is finite then the number of such cosets is referred to as the *index* of H in G, denoted by $[G\colon H]$.

The proof of Lagrange's Theorem shows that the index $[G\colon H]$ of a subgroup H of a finite group G is given by $[G\colon H] = |G|/|H|$.

Corollary 6.11. *Let x be an element of a finite group G. Then the order of x divides the order of G.*

Proof. Let H be the set of all elements of G that are of the form x^n for some integer n. Then H is a subgroup of G (see Lemma 6.5), and the order of H is the order of x. But the order of H divides G by Lagrange's Theorem (Theorem 6.10). The result follows. ∎

Corollary 6.12. *Any finite group of prime order is cyclic.*

Proof. Let G be a group of prime order, and let x be some element of G that is not the identity element. Then the order of x is greater than one and divides the order of G. But then the order of x must be equal to the order of G, since the latter is a prime number. Thus G is a cyclic group generated by x, as required. ∎

Isomorphism

Two groups are said to be *isomorphic* if the underlying algebraic structure of the two groups is the same. (We shall give a formal definition of isomorphism below.)

Example. Let C be the set consisting of the three matrices M_0, M_1 and M_2, where

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_1 = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \quad M_2 = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

Straightforward calculations show that C is a matrix group with Cayley table

	M_0	M_1	M_2
M_0	M_0	M_1	M_2
M_1	M_1	M_2	M_0
M_2	M_2	M_0	M_1 .

Now the group $\mathbb{Z}_3$ consisting of the congruence classes $[0]_3$, $[1]_3$ and $[2]_3$ of the integers 0, 1 and 2 modulo 3, with the operation of addition of congruence classes, has the Cayley table.

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$.

Examination of these two Cayley tables shows that the groups C and $\mathbb{Z}_3$ have the same algebraic structure: the element M_j of C corresponds to the element $[j]_3$ of $\mathbb{Z}_3$ for $j = 0, 1, 2$. Note that, with respect to this correspondence, the operation of matrix multiplication in C corresponds to the operation of addition in $\mathbb{Z}_3$: matrices M_i, M_j and M_k in C satisfy $M_i M_j = M_k$ if and only if $[i]_3 + [j]_3 = [k]_3$ in $\mathbb{Z}_3$. We can therefore say that the groups C and $\mathbb{Z}_3$ are isomorphic.

Example. The group D_6 of symmetries of an equilateral triangle is isomorphic to the group S_3 of permutations of a set consisting of 3 objects. This is a consequence of the fact that every permutation of the three vertices of the triangle uniquely determines a corresponding symmetry of the triangle.

An *isomorphism* from a group G to a group H is a function $\varphi\colon G \to H$ which assigns to each element x of G an element $\varphi(x)$ of H and which has the following two properties:-

- the function $\varphi\colon G \to H$ is a bijection;

- $\varphi(xy) = \varphi(x)\varphi(y)$ for all elements x and y of G.

Two groups are said to be *isomorphic* if there is an isomorphism between them. The notation '$G \cong H$' is used to denote the fact that that two groups G and H are isomorphic.

Example. Let C be the group consisting of the three matrices M_0, M_1 and M_2, where

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_1 = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \quad M_2 = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

The function sending j to M_j for $j = 0, 1, 2$ is an isomorphism from the group $\mathbb{Z}_3$ to the group C.

Example. The function which sends each permutation of the three vertices of an equilateral triangle to the corresponding symmetry of the triangle gives us an isomorphism from the group S_3 of permutations of three letters to the group D_6 of symmetries of the triangle. If the letters A, B and C label the vertices of the triangle in anticlockwise order, then the isomorphism maps the cycles $(A\,B\,C)$ and $(A\,C\,B)$ to anticlockwise rotations of the triangle through angles of $2\pi/3$ radians and $4\pi/3$ radians respectively. The isomorphism sends each transposition of $\{A, B, C\}$ to the corresponding reflection of the triangle through one of its axes of symmetry.

Example. Let C_n be a cyclic group of order n, generated by some element x. Then the function which sends x^k to $e^{2\pi ik/n}$ for each integer k is well-defined and is an isomorphism from the group C to the group of complex nth roots of unity.

Example. Let C_∞ be an infinite cyclic group generated by some element x. Each element of C_∞ is uniquely expressible in the form x^k for some integer k. (Indeed if there did exist distinct integers j and k for which $x^j = x^k$ then, for each positive integer m we would have $x^m = x^r$, where r is the remainder on dividing m by $|j - k|$, and therefore the group would be finite.) We can therefore define a function from the group C_∞ to the group $\mathbb{Z}$ of integers under addition which sends each element x^k of the group C_∞ to the integer k. It follows directly from Lemma 6.4 that this function is an isomorphism. Thus any infinite cyclic group is isomorphic to the group of integers under addition.

Normal Subgroups and Quotient Groups

Let A and B be subsets of a group G. The *product* AB of the sets A and B is defined by

$$AB = \{xy : x \in A \text{ and } y \in B\}.$$

We denote $\{x\}A$ and $A\{x\}$ by xA and Ax, for all elements x of G and subsets A of G. The Associative Law for multiplication of elements of G ensures that $(AB)C = A(BC)$ for all subsets A, B and C of G. We can therefore use the notation ABC to denote the products $(AB)C$ and $A(BC)$; and we can use analogous notation to denote the product of four or more subsets of G.

If A, B and C are subsets of a group G, and if $A \subset B$ then clearly $AC \subset BC$ and $CA \subset CB$.

Note that if H is a subgroup of the group G and if x is an element of G then xH is the left coset of H in G that contains the element x. Similarly Hx is the right coset of H in G that contains the element x.

If H is a subgroup of G then $HH = H$. Indeed $HH \subset H$, since the product of two elements of a subgroup H is itself an element of H. Also $H \subset HH$ since $h = eh$ for any element h of H, where e, the identity element of G, belongs to H.

Definition. A subgroup N of a group G is said to be a *normal subgroup* of G if $xnx^{-1} \in N$ for all $n \in N$ and $x \in G$.

The notation '$N \lhd G$' signifies 'N is a normal subgroup of G'.

Lemma 6.13. *Every subgroup of an Abelian group is a normal subgroup.*

Proof. Let N be a subgroup of an Abelian group G. Then

$$xnx^{-1} = (xn)x^{-1} = (nx)x^{-1} = n(xx^{-1}) = ne = n$$

for all $n \in N$ and $x \in G$, where e is the identity element of G. The result follows. ∎

Example. Let S_3 be the group of permutations of the set $\{1, 2, 3\}$, and let H be the subgroup of S_3 consisting of the identity permutation and the transposition $(1\,2)$. Then H is not normal in G, since $(2\,3)^{-1}(1\,2)(2\,3) = (2\,3)(1\,2)(2\,3) = (1\,3)$ and $(1\,3)$ does not belong to the subgroup H.

Proposition 6.14. *A subgroup N of a group G is a normal subgroup of G if and only if $xNx^{-1} = N$ for all elements x of G.*

Proof. Suppose that N is a normal subgroup of G. Let x be an element of G. Then $xNx^{-1} \subset N$. (This follows directly from the definition of a normal subgroup.) On replacing x by x^{-1} we see also that $x^{-1}Nx \subset N$, and thus $N = x(x^{-1}Nx)x^{-1} \subset xNx^{-1}$. Thus each of the sets N and xNx^{-1} is contained in the other, and therefore $xNx^{-1} = N$.

Conversely if N is a subgroup of G with the property that $xNx^{-1} = N$ for all $x \in G$, then it follows immediately from the definition of a normal subgroup that N is a normal subgroup of G. ∎

Corollary 6.15. *A subgroup N of a group G is a normal subgroup of G if and only if $xN = Nx$ for all elements x of G.*

Proof. Let N be a subgroup of G, and let x be an element of G. If $xNx^{-1} = N$ then $xN = (xNx^{-1})x = Nx$. Conversely if $xN = Nx$ then $xNx^{-1} = Nxx^{-1} = Ne = N$, where e is the identity element of G. Thus $xN = Nx$ if and only if $xNx^{-1} = N$. It follows from Proposition 6.14 that a subgroup N of G is normal if and only if $xN = Nx$ for all elements x of G, as required. ∎

Let N be a normal subgroup of G. Corollary 6.15 shows that a subset of G is a left coset of N in G if and only if it is a right coset of N in G. We may therefore refer to the left and right cosets of a normal subgroup N as *cosets* of N in G (since it is not in this case necessary to distinguish between left and right cosets).

Lemma 6.16. *Let N be a normal subgroup of a group G and let x and y be elements of G. Then $(xN)(yN) = (xy)N$.*

Proof. If N is a normal subgroup of G then $Ny = yN$, and therefore $(xN)(yN) = x(Ny)N = x(yN)N = (xy)(NN)$. But $NN = N$, since N is a subgroup of G. Therefore $(xN)(yN) = (xy)N$, as required. ∎

Proposition 6.17. *Let G be a group, and let N be a normal subgroup of G. Then the set of all cosets of N in G is a group under the operation of multiplication. The identity element of this group is N itself, and the inverse of a coset xN is the coset $x^{-1}N$ for any element x of G.*

Proof. Let x, y and z be any elements of G. Then the product of the cosets xN and yN is the coset $(xy)N$. The subgroup N is itself a coset of N in G, since $N = eN$. Moreover

$$(xN)N = (xN)(eN) = (xe)N = xN,$$

$$N(xN) = (eN)(xN) = (ex)N = xN,$$

$$(xN)(x^{-1}N) = (xx^{-1})N = N,$$

$$(x^{-1}N)(xN) = (x^{-1}x)N = N.$$

for all elements x of G. Thus the group axioms are satisfied. ∎

Definition. Let N be a normal subgroup of a group G. The *quotient group* G/N is defined to be the group of cosets of N in G under the operation of multiplication.

Example. Consider the dihedral group D_8 of order 8, which we represent as the group of symmetries of a square in the plane with corners at the points whose Cartesian co-ordinates are $(1, 1)$, $(-1, 1)$, $(-1, -1)$ and $(1, -1)$. Then

$$D_8 = \{\mathbf{I}, \mathbf{R}, \mathbf{R}^2, \mathbf{R}^3, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \mathbf{T}_4\},$$

where $\mathbf{I}$ denotes the identity transformation, $\mathbf{R}$ denotes an anticlockwise rotation about the origin through a right angle, and $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ and $\mathbf{T}_4$ denote the reflections in the lines $y = 0$, $x = y$, $x = 0$ and $x = -y$ respectively. Let $N = \{\mathbf{I}, \mathbf{R}^2\}$. Then N is a subgroup of D_8. The left cosets of N in D_8 are N, A, B and C, where

$$A = \{\mathbf{R}, \mathbf{R}^3\}, \qquad B = \{\mathbf{T}_1, \mathbf{T}_3\}, \qquad C = \{\mathbf{T}_2, \mathbf{T}_4\}.$$

Moreover N, A, B and C are also the right cosets of N in D_8, and thus N is a normal subgroup of D_8. On multiplying the cosets A, B and C with one another we find that $AB = BA = C$, $AC = CA = B$ and $BC = CB = A$. Therefore the quotient group D_8/N is a group of order 4 with Cayley table

	N	A	B	C
N	N	A	B	C
A	A	N	C	B
B	B	C	N	A
C	C	B	A	N .

This is the Cayley table of the *Klein 4-group* V_4.

There is an alternative approach to the construction of quotient groups which utilises the basic properties of equivalence relations. Let G be a group, and let H be a subgroup of G. Define a relation $\sim_H$ on G, where elements x and y of G satisfy $x \sim_H y$ if and only if there exists some element h of H satisfying $x = yh$. Now $x = xe$, where e, the identity element of G, is an element of H. It follows that $x \sim_H x$ for all elements x of G. Thus the relation $\sim_H$ is reflexive. If elements x and y of G satisfy $x \sim_H y$ then they also satisfy $y \sim_H x$, for if $x = yh$, where h is an element of H, then $y = xh^{-1}$. Thus the relation $\sim_H$ is symmetric. If x, y and z are elements of G satisfying $x \sim_H y$ and $y \sim_H z$ then $x \sim_H z$, for if $x = yh$ and $y = zk$, where h and k belong to H, then $x = zkh$, and kh belongs to H. Thus the relation $\sim_H$ is transitive. We conclude that the relation $\sim_H$ is an equivalence relation. One can readily verify that its equivalence classes are the left cosets of H in G.

Now suppose that the subgroup H is normal in G. Let x, y, u and v be elements of G, where $x \sim_H u$ and $y \sim_H v$. Then there exist elements h and k of H such that $x = uh$ and $y = vk$. Then

$xy = uhvk = uv(v^{-1}hvk)$. Now $v^{-1}hv \in H$ since $h \in H$ and H is normal in G. It follows that $v^{-1}hvk \in H$, since the product of any two elements of a subgroup belongs to that subgroup. We deduce that if $x \sim_H u$ and $y \sim_H v$ then $xy \sim_H uv$. Also $x^{-1} = (uh)^{-1} = h^{-1}u^{-1} = u^{-1}(uh^{-1}u^{-1}$, where $uh^{-1}u^{-1} \in H$. It follows that if $x \sim_H u$ then $x^{-1} \sim_H u^{-1}$.

Now, for any $x \in G$, let C_x denote the coset of H to which the element x belongs. Now C_x is the equivalence class of x with respect to the equivalence relation $\sim_H$. It follows from this that elements x and u satisfy $C_x = C_u$ if and only if $x \sim_H u$. We conclude that if H is normal in G, and if $C_x = C_u$ and $C_y = C_v$ then $C_{xy} = C_{uv}$ and $C_{x^{-1}} = C_{u^{-1}}$. One can deduce from this that there is a well-defined group multiplication operation on cosets of H in G, where C_xC_y is defined to be C_{xy}. The results just prove show that this definition of C_xC_y does not depend on the choice of x and y representing their respective cosets. The identity element is the subgroup H itself, which can be viewed as the coset containing the identity element, and the inverse of the coset C_x is the coset $C_{x^{-1}}$. One can readily verify that all the group axioms are satisfied and thus the set of cosets of H in G does indeed constitute a group, the quotient group G/H.

Homomorphisms

Definition. A homomorphism $\theta\colon G \to K$ from a group G to a group K is a function with the property that $\theta(g_1 * g_2) = \theta(g_1) * \theta(g_2)$ for all $g_1, g_2 \in G$, where $*$ denotes the group operation on G and on K.

Example. Let $\mathbb{Z}$ be the group of integers (with the operation of addition). The function $\theta\colon \mathbb{Z} \to \mathbb{Z}$ that sends each integer n to $2n$ is a homomorphism. This follows from the fact that $2(m+n) = 2m+2n$ for all integers m and n. More generally, given any integer q, the function that sends each integer n to qn is a homomorphism.

Example. There is an obvious homomorphism from the group of integers to the group of real numbers (where the group operation for both groups is addition). This is the homomorphism that sends each integer to itself.

Example. Let a be a positive real number. The function that sends each integer n to the real number a^n is a homomorphism from the group of integers (with the operation of addition) to the group of non-zero real numbers (with the operation of multiplication). This follows from the fact that $a^{m+n} = a^m a^n$ for all integers m and n.

Example. Let g be an element of a group G, and let $\varphi\colon \mathbb{Z} \to G$ be defined by $\varphi(n) = g^n$ for all integers n. The fact that $g^{m+n} = g^m g^n$ for all integers m and n ensures that the function $\varphi\colon \mathbb{Z} \to G$ is a homomorphism from the group of integers (with the operation of addition) to the given group G.

Example. Let U be the group of complex numbers z satisfying $|z| = 1$ (with the operation of multiplication). There is a homomorphism $\psi\colon \mathbb{R} \to U$ defined by $\psi(x) = \exp(2\pi i x)$ for all real numbers x (where $\mathbb{R}$ is the group of real numbers with the operation of addition). Indeed

$$\psi(x+y) = \exp(2\pi i(x+y)) = \exp(2\pi i x)\exp(2\pi i y) = \psi(x)\psi(y)$$

for all real numbers x and y.

Example. Let S_n be the group of all permutations of a set of n objects, Then there is a homomorphism $\epsilon\colon S^n \to \{+1, -1\}$, where the group operation on the set $\{+1, -1\}$ is multiplication. This homomorphism is defined by the requirement that $\epsilon(\sigma) = +1$ when the permutation σ is even, and $\epsilon(\sigma) = -1$ when the permutation σ is odd. The fact that $\epsilon\colon S^n \to \{+1, -1\}$ is a homomorphism follows from the following results: the composition of two even permutations is even; the composition of two odd permutations is even; the composition of an even permutation and an odd permutation (in any order) is odd.

Lemma 6.18. *Let $\theta\colon G \to K$ be a homomorphism. Then $\theta(e_G) = e_K$, where e_G and e_K denote the identity elements of the groups G and K. Also $\theta(x^{-1}) = \theta(x)^{-1}$ for all elements x of G.*

Proof. Let $z = \theta(e_G)$. Then $z^2 = \theta(e_G)\theta(e_G) = \theta(e_G e_G) = \theta(e_G) = z$. The result that $\theta(e_G) = e_K$ now follows from the fact that an element z of K satisfies $z^2 = z$ if and only if z is the identity element of K.

Let x be an element of G. The element $\theta(x^{-1})$ satisfies $\theta(x)\theta(x^{-1}) = \theta(xx^{-1}) = \theta(e_G) = e_K$, and similarly $\theta(x^{-1})\theta(x) = e_K$. The uniqueness of the inverse of $\theta(x)$ now ensures that $\theta(x^{-1}) = \theta(x)^{-1}$. ▮

An *isomorphism* $\theta\colon G \to K$ between groups G and K is a homomorphism that is also a bijection mapping G onto K. Two groups G and K are *isomorphic* if there exists an isomorphism mapping G onto K.

Example. Let D_6 be the group of symmetries of an equilateral triangle in the plane with vertices A, B and C, and let S_3 be the group of permutations of the set $\{A, B, C\}$. The function which sends a symmetry of the triangle to the corresponding permutation of its vertices is an isomorphism between the dihedral group D_6 of order 6 and the symmetric group S_3.

Example. Let $\mathbb{R}$ be the group of real numbers with the operation of addition, and let $\mathbb{R}^+$ be the group of strictly positive real numbers with the operation of multiplication. The function $\exp\colon \mathbb{R} \to \mathbb{R}^+$ that sends each real number x to the positive real number e^x is an isomorphism: it is both a homomorphism of groups and a bijection. The inverse of this isomorphism is the function $\log\colon \mathbb{R}^+ \to \mathbb{R}$ that sends each strictly positive real number to its natural logarithm.

Here is some further terminology regarding homomorphisms:

- A *monomorphism* is an injective homomorphism.
- An *epimorphism* is a surjective homomorphism.
- An *endomorphism* is a homomorphism mapping a group into itself.
- An *automorphism* is an isomorphism mapping a group onto itself.

Definition. The *kernel* $\ker\theta$ of the homomorphism $\theta\colon G \to K$ is the set of all elements of G that are mapped by θ onto the identity element of K.

Example. Let the group operation on the set $\{+1, -1\}$ be multiplication, and let $\theta\colon \mathbb{Z} \to \{+1, -1\}$ be the homomorphism that sends each integer n to $(-1)^n$. Then the kernel of the homomorphism θ is the subgroup of $\mathbb{Z}$ consisting of all even numbers.

Example. Let S_n be the group of all permutations of a set of n objects, let the group operation on the set $\{+1, -1\}$ be multiplication, and let $\epsilon\colon S_n \to \{+1, -1\}$ be the homomorphism that sends each permutation σ in S_n to $\epsilon(\sigma)$, where $\epsilon(\sigma) = +1$ if the permutation σ is even and $\epsilon(\sigma) = -1$ if the permutation σ is odd. Then the kernel of the homomorphism $\epsilon\colon S_n \to \{+1, -1\}$ is the group of all even permutations of the set of n objects.

Lemma 6.19. *Let G and K be groups, and let $\theta\colon G \to K$ be a homomorphism from G to K. Then the kernel* $\ker\theta$ *of θ is a normal subgroup of G.*

Proof. Let x and y be elements of $\ker\theta$. Then $\theta(x) = e_K$ and $\theta(y) = e_K$, where e_K denotes the identity element of K. But then $\theta(xy) = \theta(x)\theta(y) = e_K e_K = e_K$, and thus xy belongs to $\ker\theta$. Also $\theta(x^{-1}) = \theta(x)^{-1} = e_K^{-1} = e_K$, and thus x^{-1} belongs to $\ker\theta$. We conclude that $\ker\theta$ is a subgroup of K. Moreover $\ker\theta$ is a normal subgroup of G, for if $g \in G$ and $x \in \ker\theta$ then

$$\theta(gxg^{-1}) = \theta(g)\theta(x)\theta(g)^{-1} = \theta(g)\theta(g^{-1}) = e_K. \quad \blacksquare$$

If N is a normal subgroup of some group G then N is the kernel of the *quotient homomorphism* $\theta\colon G \to G/N$ that sends $g \in G$ to the coset gN. It follows therefore that a subset of a group G is a normal subgroup of G if and only if it is the kernel of some homomorphism.

Proposition 6.20. *Let G and K be groups, let $\theta\colon G \to K$ be a homomorphism from G to K, and let N be a normal subgroup of G. Suppose that $N \subset \ker\theta$. Then the homomorphism $\theta\colon G \to K$ induces a homomorphism $\hat\theta\colon G/N \to K$ sending $gN \in G/N$ to $\theta(g)$. Moreover $\hat\theta\colon G/N \to K$ is injective if and only if $N = \ker\theta$.*

Proof. Let x and y be elements of G. Now $xN = yN$ if and only if $x^{-1}y \in N$. Also $\theta(x) = \theta(y)$ if and only if $x^{-1}y \in \ker\theta$. Thus if $N \subset \ker\theta$ then $\theta(x) = \theta(y)$ whenever $xN = yN$, and thus $\theta\colon G \to K$ induces a well-defined function $\hat\theta\colon G/N \to K$ sending $xN \in G/N$ to $\theta(x)$. This function is a homomorphism, since $\hat\theta((xN)(yN)) = \hat\theta(xyN) = \theta(xy) = \theta(x)\theta(y) = \hat\theta(xN)\hat\theta(yN)$.

Suppose now that $N = \ker\theta$. Then $\theta(x) = \theta(y)$ if and only if $xN = yN$. Thus the homomorphism $\hat\theta\colon G/N \to K$ is injective. Conversely if $\hat\theta\colon G/N \to K$ is injective then N must be the kernel of θ, as required. $\blacksquare$

Corollary 6.21. *Let G and K be groups, and let $\theta\colon G \to K$ be a homomorphism. Then $\theta(G) \cong G/\ker\theta$.*

Example. Let S_n be the group of all permutations of a set of n objects, let A_n be the subgroup of S_n consisting of all even permutations of those objects, and let the group operation on the set $\{+1, -1\}$ be multiplication. Then $S_n/A_n \cong \{+1, -1\}$. This follows from the fact that A_n is the kernel of the homomorphism $\epsilon\colon S_n \to \{+1, -1\}$ that sends each permutation σ in S_n to $\epsilon(\sigma)$, where $\epsilon(\sigma) = +1$ if the permutation σ is even and $\epsilon(\sigma) = -1$ if the permutation σ is odd.

The Isomorphism Theorems

Lemma 6.22. *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then the set HN is a subgroup of G, where $HN = \{hn : h \in H \text{ and } n \in N\}$.*

Proof. The set HN clearly contains the identity element of G. Let x and y be elements of HN. We must show that xy and x^{-1} belong to HN. Now $x = hu$ and $y = kv$ for some elements h and k of H and for some elements u and v of N. Then $xy = (hk)(k^{-1}ukv)$. But $k^{-1}uk \in N$, since N is normal. It follows that $k^{-1}ukv \in N$, since N is a subgroup and $k^{-1}ukv$ is the product of the elements $k^{-1}uk$ and v of N. Also $hk \in H$. It follows that $xy \in HN$.

We must also show that $x^{-1} \in HN$. Now $x^{-1} = u^{-1}h^{-1} = h^{-1}(hu^{-1}h^{-1})$. Also $h^{-1} \in H$, since H is a subgroup of G, and $hu^{-1}h^{-1} \in N$, since N is a normal subgroup of G. It follows that $x^{-1} \in HN$, and thus HN is a subgroup of G, as required. $\blacksquare$

Theorem 6.23. (First Isomorphism Theorem) *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then*

$$\frac{HN}{N} \cong \frac{H}{N \cap H}.$$

Proof. Every element of HN/N is a coset of N that is of the form hN for some $h \in H$. Thus if $\varphi(h) = hN$ for all $h \in H$ then $\varphi\colon H \to HN/N$ is a surjective homomorphism, and $\ker \varphi = N \cap H$. But $\varphi(H) \cong H/\ker\varphi$ (Corollary 6.21). Therefore $HN/N \cong H/(N \cap H)$ as required. ▮

Theorem 6.24. (Second Isomorphism Theorem) *Let M and N be normal subgroups of a group G, where $M \subset N$. Then*

$$\frac{G}{N} \cong \frac{G/M}{N/M}.$$

Proof. There is a well-defined homomorphism $\theta\colon G/M \to G/N$ that sends gM to gN for all $g \in G$. Moreover the homomorphism θ is surjective, and $\ker\theta = N/M$. But $\theta(G/M) \cong (G/M)/\ker\theta$ (Corollary 6.21). Therefore G/N is isomorphic to $(G/M)\,/\,(N/M)$, as required. ▮

Direct products of groups

Let $G_1, G_2, \ldots, G_n$ be groups, and let G be the Cartesian product $G_1 \times G_2 \times \cdots \times G_n$ of $G_1, G_2, \ldots, G_n$ (when the latter are regarded as sets). Then the elements of G are n-tuples $(x_1, x_2, \ldots, x_n)$ where $x_i \in G_i$ for $i = 1, 2, \ldots, n$. We can multiply two elements of G as follows:

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

One can readily verify that G is a group with respect to this binary operation: multiplication is associative; the identity element of the group is $(e_1, e_2, \ldots, e_n)$, where e_i is the identity element of G_i for each i; and the inverse of an element $(x_1, x_2, \ldots, x_n)$ of G is $(x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1})$. We say that the group G is the *direct product* of the groups $G_1, G_2, \ldots, G_n$: this direct product is (not surprisingly) denoted by $G_1 \times G_2 \times \cdots \times G_n$.

Example. Let C_2 and C_3 be cyclic groups of orders 2 and 3 respectively. Then $C_2 \times C_3$ is a cyclic group of order 6, and $C_2 \times C_2$ is isomorphic to the Klein 4-group whose Cayley table is

	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I .

Let us first consider $C_2 \times C_3$. Let x and y be generators of C_2 and C_3 respectively, and let e and e' denote the identity elements of C_2 and C_3. Thus $C_2 = \{e, x\}$ and $C_3 = \{e', y, y^2\}$, where $x^2 = e$ and $y^3 = e'$. The elements of $C_2 \times C_3$ are

$$(e, e'), \quad (e, y), \quad (e, y^2), \quad (x, e'), \quad (x, y), \quad (x, y^2).$$

Let $z = (x, y)$. On computing the powers of z we find that

$$z^2 = (e, y^2), \quad z^3 = (x, e'), \quad z^4 = (e, y), \quad z^5 = (x, y^2), \quad z^6 = (e, e').$$

Thus 6 is the smallest positive integer n for which z^n is equal to the identity element (e, e') of the group. We deduce that the group $C_2 \times C_3$ (which is a group of order 6) must be a cyclic group generated by the element z.

Next consider $C_2 \times C_2$. This has four elements I, A, B and C, where $I = (e, e)$, $A = (e, x)$, $B = (x, e)$ and $C = (x, x)$. If we calculate the Cayley table for the group, we discover that it is that of the Klein 4-group.

Cayley's Theorem

Theorem 6.25. (Cayley's Theorem) *Let G be a group of order n. Then G is isomorphic to a subgroup of the group S_n of permutations of a set of n elements.*

Proof. For each element x of G, let $\sigma_x: G \to G$ be the function defined such that $\sigma_x(g) = xg$ for all $g \in G$. Now

$$\sigma_{x^{-1}}(\sigma_x(g)) = x^{-1}(xg) = (x^{-1}x)g = g$$

and

$$\sigma_x(\sigma_{x^{-1}}(g)) = x(x^{-1}g) = (x(x^{-1})g = g$$

for all $g \in G$. It follows that, for any $x \in G$, the function $\sigma_x: G \to G$ is a bijection whose inverse is $\sigma_{x^{-1}}$ It follows that σ_x is a permutation of G for all $x \in G$, and thus the function sending an element x of G to the permutation σ_x is a function from G to the group of permutations of G. This function is a homomorphism. Indeed $\sigma_{xy} = \sigma_x \circ \sigma_y$ since $\sigma_{xy}(g) = (xy)g = x(yg) = \sigma_x(\sigma_y(g))$ for all $g \in G$. The homomorphism sending $x \in G$ to σ_x is be injective, for if σ_x is the identity permutation then $xg = g$ for all $g \in G$, and hence x is the identity element of G. It follows that G is isomorphic to the image of the homomorphism. This image is a subgroup $\{\sigma_x : x \in G\}$ of the group of permutations of G. The result follows. ▮

Problems

1. Calculate the Cayley table for the dihedral group D_8 of order 8 (i.e., the symmetry group of a square).

2. Find all subgroups of the dihedral group of order 8, and calculate also all left and right cosets of those subgroups. Which subgroups are normal subgroups?

3. Let G be a set with a binary operation $*$, associating to each pair of elements x and y of G a third element $x * y$ of G. Suppose that the following properties are satisfied:

   - $(x * y) * z = x * (y * z)$ for all elements x, y, and z of G (the *Associative Law*);
   - there exists an element e of G such that $e * x = x$ for all elements x of G;
   - for each element x of G there exists an element x' of G satisfying $x' * x = e$.

   Prove that G is a group with respect to this binary operation. [Thus you must show that $x * e = x$ and $x * x' = e$ for all $x \in G$.]

4. Prove that a non-empty subset H of a group G is a subgroup of G if and only if $xy^{-1} \in H$ for all $x \in H$ and $y \in H$.

5. Let G be a group. Prove that any subgroup N of index 2 in G is a normal subgroup of G.

6. Let G be a group and let H be a subgroup of G. Show that the function mapping G onto itself that sends $g \in G$ to g^{-1} induces a bijection from the set of left cosets of H in G to the set of right cosets of H in G. Hence show that the number of left cosets of H is equal to number of right cosets of H, if either of these numbers is finite.

7. Let G be a group. The *centre* $Z(G)$ of G is defined by

$$Z(G) = \{z \in G : gz = zg \text{ for all } g \in G\}.$$

Prove that the centre $Z(G)$ of a group G is a normal subgroup of G. [In particular, you should show that $Z(G)$ is a subgroup of G.]