

# 4. FIRST STEPS IN THE THEORY

## §4.1. A Catalogue of All Groups: The Impossible Dream

The fundamental problem of group theory is to systematically explore the landscape and to chart what lies out there. We'd like to have a catalogue of all groups, or perhaps just all finite groups: a catalogue which would provide one specimen of each group so that we'd be able to say that every group (or every finite group) is isomorphic to exactly one of the specimens in the catalogue. In particular we'd know exactly how many groups there are of any given order.

This is an impossible dream, but not simply because there are infinitely many finite groups. After all there are infinitely many finite-dimensional vector spaces over a given field yet we can describe them all in a single statement: every finite-dimensional vector space over a field  $F$  is isomorphic to the space of  $n$ -tuples  $(x_1, x_2, \dots, x_n)$  over  $F$  for some  $n$ . This is just a corollary of the theorem that every finite-dimensional vector space has a basis. In other words there's exactly one vector space over  $F$  (up to isomorphism) for each dimension.

Structure theorems exist in various parts of mathematics. We know all the finite fields. In topology the compact surfaces are all known. Within group theory itself we have a number of classification theorems. For example we know all the finite abelian groups, via the Fundamental Theorem of Abelian Groups that we prove in a later chapter.

The most celebrated example is the classification of all finite "simple" groups. Don't worry now what a simple group is. In a certain sense they're the building blocks for all finite groups but the term "simple" is deceptive. They're not the most elementary of groups but their simplicity refers to the fact that they can't be pulled apart, in a certain way, into smaller groups. They're the atoms of the universe of finite groups.

Now this celebrated theorem is the culmination of virtually a century's work by many thousands of group theorists and its proof is scattered over numerous research journals in the literature. It has never been assembled in one place because it's estimated that it would occupy about 20,000 pages and because of this it even made it to the Guinness Book of Records!

The goal of this chapter is to develop enough of the theory to enable us to prove a couple of classification theorems. Nothing so ambitious as the one we were just talking about. Just a couple of nice, gentle theorems. Together they describe, for each prime  $p$ , the groups of order  $p$  and of order  $2p$ . There aren't very many such groups for a given prime. In fact there's only one group of order  $p$  and just two of order  $2p$ . So contrary to what you might expect the number of different groups doesn't grow steadily with the group order. The groups of order 32 have been catalogued and there are over 50 of them. But there's only one group of order 31 because 31 is prime and there are just two groups of order 34.

## §4.2. Additive and Multiplicative Notation

Until now we've written the combination of  $a$  and  $b$  in an abstract group as  $a * b$ . But, unless there's danger of confusion, it's more usual to write the binary operation as if it was addition or multiplication.

If we're proving theorems about abstract groups in general, where the group could be non-abelian, we use **multiplicative notation**. If the groups we're considering are all abelian we frequently use **additive notation**. The reason for this distinction is that we're used to multiplication being non-commutative (for example matrices and permutations), but in all the systems we've encountered, addition is always commutative. It's very dangerous therefore to use additive notation in a non-commutative group.

GENERAL NOTATION	MULTIPLICATIVE NOTATION	ADDITIVE NOTATION
$a * b$	$ab$	$a + b$
$a * a * \dots * a$	$a^n$	$na$
$e$	$1$	$0$
inverse of $a$	$a^{-1}$	$-a$

Unless otherwise stated, we'll use multiplicative notation.

## §4.3. Basic Properties of Groups

**Theorem 1: The identity element of a group is unique.**

**Proof:** Suppose  $e, f$  are identities for a group  $G$ . Then  $e = e f$  (since  $f$  is an identity)  $= f$  (since  $e$  is an identity).

**Theorem 2: Each element of a group has only one inverse.**

**Proof:** Suppose  $b, c$  are both inverses of the element  $a$  in a group  $G$ . Then  $b = b1 = b(ac) = (ba)c = 1c = c$ .

**Theorem 3: (Cancellation Law) If  $ax = ay$  then  $x = y$ .**

**Proof:** Suppose  $ax = ay$ . Then  $a^{-1}(ax) = a^{-1}(ay)$ .

Hence  $(a^{-1}a)x = (a^{-1}a)y$ . Thus  $1x = 1y$  and so  $x = y$ .

Notice that all the group axioms (except the Closure Law) are needed to prove this.

Similarly one can prove that  $xa = ya$  implies that  $x = y$ . Thus cancellation on the left, or on the right, is possible. A consequence of the cancellation law is that:

**For a finite group every element appears exactly once and only once in each row and column of the multiplication table.**

You should take careful note of the fact that you can't cancel on the left-hand end of one side of the equation and on the right-hand end of the other. So  $ax = xb$  needn't imply that  $a = b$  (unless the group is abelian).

## §4.4. Powers

If  $g$  is an element of a group, we define positive integer powers of  $g$  inductively as follows:

$$g^0 = 1;$$

$$g^{n+1} = g^n g \text{ for all } n \geq 0.$$

We define negative powers by  $g^{-n} = (g^{-1})^n$  for all negative integers  $-n$ .

**Theorem 4:** For all natural numbers  $m, n$  and all elements  $a, b$  in a group  $G$ :

- (1)  $a^m a^n = a^{m+n}$ ;
- (2)  $(a^m)^n = a^{mn}$ ;
- (3) if  $G$  is abelian,  $(ab)^n = a^n b^n$ ;
- (4)  $(b^{-1}ab)^n = b^{-1}a^n b$ .

**Proof:** Although these seem obvious enough (and indeed they are obvious if  $m$  and  $n$  are positive, just by counting factors) the cases where one or both are negative require special attention.

(1) This is obvious if both  $m, n$  are positive or zero. Suppose  $m$  is positive and  $n$  is negative, say  $n = -r$ . If  $m \geq r$  then on the left hand side there will be  $r$  cancelling pairs of  $aa^{-1}$  leaving  $m - r = m + n$  factors. If  $m < r$  there will be only  $m$  such pairs leaving  $r - m$  factors of  $a^{-1}$ . The result is therefore  $a^{-(r-m)} = a^{m-r} = a^{m+n}$ .

We've thus proved the result for all  $n$  where  $m \geq 0$ . If  $m$  is negative, say  $m = -s$ , then putting  $b = a^{-1}$  the left hand side is  $b^s b^{-n}$ . By the earlier case this is  $b^{s-n} = a^{n-s} = a^{m+n}$ .

(2) Again this is obvious if  $m, n$  are both positive. The other cases are left as an exercise.

(3) If  $n$  is positive we simply count the number of factors on each side. Because the group is assumed to be abelian the factors may be rearranged so all the  $a$ 's can be brought to the front. If  $n$  is zero, LHS = RHS = 1. If  $n$  is negative we put  $b = a^{-1}$  and use the positive case.

(4) If  $n$  is positive,  $(b^{-1}ab)^n = b^{-1}(bb^{-1})a(bb^{-1}) \dots (bb^{-1})ab$  ( $n$  factors)  $= b^{-1}aa \dots ab = b^{-1}a^n b$ . If  $n = 0$ , LHS = RHS = 1. If  $n$  is negative we use the positive case on  $b^{-1}cb$  where  $c$  is defined to be  $a^{-1}$ .

**Theorem 5:** In a group  $G$   $(ab)^{-1} = b^{-1}a^{-1}$ .

**Proof:**  $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = 1$  and similarly  $(ab)(b^{-1}a^{-1}) = 1$ .

Remember that the inverse of a product is the product of the inverses **in reverse order**.

The **cyclic subgroup** generated by an element  $g$  is the set of all powers of  $g$  (including 1 as  $g^0$  and negative powers). It's denoted by  $\langle g \rangle$ .

**Definition:** The **order** of an element  $g$  of a group is the smallest positive integer  $n$  such that  $g^n = 1$ . In additive notation this becomes  $ng = 0$ .

The order of  $g$  is denoted by  $|g|$ . If there's no such positive  $n$ , we say that  $g$  has **infinite order**.

For example the order of  $i$  in the group of non-zero complex numbers under multiplication is 4, and the integer 2 has infinite order. The identity element of any group is the only element of order 1.

**Theorem 6: The order of an element  $g \in G$  is at most  $|G|$ .**

**Proof:** Let  $n = |G|$ . The elements  $1, g, g^2, \dots, g^{n-1}, g^n$  can't be distinct (there are  $n+1$  of them in a group of order  $n$ ). Hence there must be some repetition:  $g^r = g^s$  for some  $r, s$  with  $0 \leq r < s \leq n$ . Thus  $g^{s-r} = 1$  and since  $0 < r < s \leq n$ ,  $|g| \leq n$ .

**Theorem 7: Groups of even order must contain an element of order 2.**

**Proof:** Suppose  $|G|$  is even. Now the elements of  $G$  which differ from their inverses must come in pairs  $\{x, x^{-1}\}$ . Since  $|G|$  is even, the remaining elements, those for which  $x = x^{-1}$ , must also be even in number. But  $x = x^{-1}$  is equivalent to  $x^2 = 1$  and so these are the elements of order 2, together with the identity. Leaving out the identity, there must be an odd number of elements of order 2 and so the number of elements of order 2 must be at least 1.

**Theorem 8: If all of the elements of  $G$  (except 1) have order 2, then  $G$  must be abelian.**

**Proof:** Let  $x, y \in G$ . Then  $(xy)^2 = 1$ . But also  $x^2y^2 = 1$  and so  $xyxy = xxyy$ .

Multiplying by  $x^{-1}$  on the left and by  $y^{-1}$  on the right of each side of the equation we conclude that  $yx = xy$ . Since this holds for all  $x, y \in G$  it follows that  $G$  is abelian.

## §4.5. Cyclic Groups

A group  $G$  is **cyclic** if it can be generated by a single element, that is if  $G = \langle g \rangle$  for some  $g \in G$ .

### Example 1:

The set of  $n$ -th roots of unity,  $G = \{z \in \mathbf{C} \mid z^n = 1\}$ , is a group under multiplication. It is a cyclic group because it can be generated by  $e^{2\pi i/n}$ . This is because every  $n$ -th root of 1 has the form  $e^{2k\pi i/n} = (e^{2\pi i/n})^k$ . In particular the group of 4-th roots of unity is  $\{1, i, -1, -i\}$  which is generated by  $i$ .

### Example 2:

The group of symmetries of a parallelogram is  $\{I, R\}$  where  $R$  is a  $180^\circ$  rotation about its centre. This group is thus generated by  $R$ .

### Example 3:

The group  $(\mathbf{Z}, +)$  of integers under addition is cyclic because it can be generated by the integer 1. Remember that we're using additive notation here so instead of saying that every integer is an integer power of 1 (which is not the case), we should be saying that every integer is an integer *multiple* of 1 (which it is). Note that  $-1$  also generates this group, but  $\pm 1$  are the only generators.

**Theorem 9: Cyclic groups are abelian.**

**Proof:** Two typical elements in the cyclic group  $\langle g \rangle$  are  $g^r$  and  $g^s$ . Now  $g^r g^s = g^{r+s} = g^s g^r$ . So every pair of elements commute and hence the cyclic group is abelian.

**Theorem 10:** A finite group of order  $n$  is cyclic if and only if it contains an element of order  $n$ .

**Proof:** If  $|G| = n$  and  $G$  has an element  $g$  of order  $n$  then  $\langle g \rangle$ , the cyclic subgroup generated by  $g$  has order  $n$  (ie. there are  $n$  distinct powers of  $g$ ). Thus there are no other elements in  $G$ . They're all powers of  $g$  and so  $g$  is a generator for  $G$  and hence  $G$  is cyclic.

Conversely suppose that  $G$  is a cyclic group of order  $n$ . Then if  $g$  is a generator,  $g$  must have order  $n$ .

**Example 4:**

The group given by the following multiplication table is not cyclic since it has no element of order 4.

	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

### §4.6. Subgroups

If  $G$  is a group and  $H$  is a subset of  $G$  then  $H$  is a **subgroup** if

- (1)  $xy \in H$  for all  $x, y \in H$
- (2)  $1 \in H$
- (3)  $x^{-1} \in H$  for all  $x \in H$ .

A subgroup  $H$  is a group in its own right. Every group is a subgroup of itself. All other subgroups are called **proper subgroups**. The **trivial subgroup**,  $1 = \{1\}$  is a subgroup of any group.

**Notation:**  $H \leq G$  means " $H$  is a subgroup of  $G$ " and  $H < G$  means " $H$  is a *proper* subgroup of  $G$ " ie.  $H$  is a subgroup but is not  $G$  itself.

**Example 5:**  $2Z$  (the group of even integers) is a subgroup of  $Z$  (under  $+$ ).

**Theorem 11:** For all  $g \in G$ ,  $\langle g \rangle$  is a subgroup of  $G$ .

**Proof:** For all  $r, s \in Z^+$ ,  $g^r g^s = g^{r+s} \in \langle g \rangle$ ;  $1 = g^0 \in \langle g \rangle$  and for all  $r$ ,  $(g^r)^{-1} = g^{-r} \in \langle g \rangle$ .

### §4.7. Cosets and Lagrange's Theorem

Let  $H \leq G$ . Define a relation  $\equiv$  by defining  $x \equiv y$  if  $x = yh$  for some  $h \in H$ .

**Theorem 12:**  $\equiv$  is an equivalence relation.

**Proof:** *Reflexive* Let  $a \in G$ . Then  $a = a1$ . Since  $1 \in H$ ,  $a \equiv a$ .

*Symmetric* Suppose  $a \equiv b$ . Then  $a = bh$  for some  $h \in H$ . Hence  $ah^{-1} = b$ . Since  $h^{-1} \in H$ ,  $b \equiv a$ .

*Transitive* Suppose  $a \equiv b$  and  $b \equiv c$ . Then  $a = bh$  for some  $h \in H$  and  $b = ck$  for some  $k \in H$ .

Thus  $a = (ck)h = c(kh)$ . Since  $kh \in H$ ,  $a \equiv c$ .

**NOTE:** Each of the three properties of an equivalence relation comes from one of the three closure properties of a subgroup.

The equivalence classes under  $\equiv$  are called the **right cosets** of  $H$  in  $G$ .

**Notation:**  $gH$  denotes the right coset containing  $g$ .

**NOTE:** Left cosets are defined similarly.

**Example 6:**  $G = \mathbf{R}^\#$ ,  $H = \{\pm 1\}$  under the operation of multiplication. The cosets are all of the form  $\{\pm x\}$ .

**Example 7:**  $G = \mathbf{C}^\#$ , the group of non-zero complex numbers under multiplication and let  $H$  be the set of all complex numbers with modulus 1. The right (or left) cosets of  $H$  in  $G$  are all the circles with centre  $O$ .

**Example 8:** Suppose  $G = S_3$  and  $H = \{I, (12)\}$ . The left and right cosets of  $H$  in  $G$  are:

$$\begin{aligned} HI &= \{II, (12)I\} = \{I, (12)\} & IH &= \{II, I(12)\} = \{I, (12)\} \\ H(13) &= \{I(13), (12)(13)\} = \{(13), (123)\} & (13)H &= \{(13)I, (13)(12)\} = \{(13), (132)\} \\ H(23) &= \{I(23), (12)(23)\} = \{(23), (132)\} & (23)H &= \{(23)I, (23)(12)\} = \{(23), (123)\}. \end{aligned}$$

Notice that in this case, left and right cosets are different.

**Example 9:**  $G = S_3$ ,  $H = \{I, (123), (132)\}$ . Here the left and right cosets give the same decomposition of  $G$ . These two (left/right) cosets are  $H$  itself and  $\{(12), (13), (23)\}$ .

### Theorem 13:

(1) The subgroup  $H$  is itself one of the cosets of  $H$  in  $G$ .

(2) Two elements  $a, b$  belong to the same right coset (of  $H$  in  $G$ ) if and only if  $b^{-1}a \in H$ .

**Proof:** (1)  $H = 1H$ .

(2)  $a, b$  belong to the same right coset  $\Leftrightarrow a \equiv b \Leftrightarrow a = bh$  for some  $h \in H \Leftrightarrow b^{-1}a = h$  for some  $h \in H \Leftrightarrow b^{-1}a \in H$ .

Equivalence classes can be of different sizes, but for cosets, they must have the same size.

**Theorem 14:** If  $H \leq G$ , every coset of  $H$  in  $G$  has  $|H|$  elements.

**Proof:** There's a natural 1-1 correspondence between any coset  $aH$  and  $H$  itself viz.  $ah \leftrightarrow h$ . Hence the number of elements in each is the same.

**Theorem 15: (Lagrange) The order of a subgroup (of a finite group) divides the order of the group.**

**Proof:** Suppose there are  $m$  cosets of  $H$  in  $G$ . Since  $G$  is the disjoint union of them and each coset has  $|H|$  elements, it follows that  $|G| = m \cdot |H|$  and so  $|H|$  divides  $|G|$ .

This is a very powerful result. It shows that the number of elements in a group greatly affects its structure.

**Example 10:** If  $|G| = 14$ , the only possible orders for a subgroup are 1, 2, 7 and 14.

**Theorem 16: Groups of prime order are cyclic.**

**Proof:** Suppose  $|G| = p$  where  $p$  is prime.

Since  $p \geq 2$  we may choose  $g \in G$  such that  $g \neq 1$ . Let  $H = \langle g \rangle$ .

Let  $|H| = n$ . Now  $n \mid p$  and  $n > 1$  so  $n = p$ . Hence  $G = H$  and so is cyclic.

Since the order of an element is the order of the cyclic subgroup it generates, we have:

**Theorem 17: The order of an element of a finite group divides the order of the group.**

## §4.8. Dihedral Groups

The family of cyclic groups contains those groups with the simplest possible group structure. A closely related family is the family of dihedral groups.

**Definition:** The dihedral group of order  $2n$  is the group:

$$D_{2n} = \langle A, B \mid A^n = 1, B^2 = 1, BA = A^{-1}B \rangle.$$

Dihedral groups occur naturally in many different guises.  $D_{2n}$  is, for example, the group structure of the symmetry group of a regular  $n$ -sided polygon. The symmetry operations consist of the rotation  $R$  through  $2\pi/n$ , and its powers plus the  $180^\circ$  rotations about the  $n$  axes of symmetry. But if  $Q$  denotes any one of these, the others can be expressed in the form  $R^kQR^{-k}$ .

If, for example, there is a vertical axis of symmetry and  $Q$  denotes the  $180^\circ$  degree rotation about it, any other  $180^\circ$  symmetry operation can be achieved by rotating the axis until it becomes vertical ( $R^k$ ), carrying out  $Q$  about the vertical axis, and then rotating the axis back to its original position ( $R^{-k}$ ).

Now  $R^n = 1$  ( $n$  successive rotations through  $2\pi/n$ );

$Q^2 = 1$  (two successive  $180^\circ$  rotations) and

$QRQ = R^{-1}$  (a negative or clockwise rotation can be achieved by rotating about the vertical axis first, then rotating in the positive direction and finally rotating back in the vertical axis – try it!) and so  $RQ = QR^{-1}$ .

So this symmetry group is  $\langle R, Q \mid R^n = 1, Q^2 = 1, RQ = QR^{-1} \rangle$ , that is, it is the dihedral group of order  $2n$ . In particular  $D_8$  is the symmetry group of a square.

## §4.9. Dihedral Arithmetic

The dihedral group  $D_{2n} = \langle A, B \mid A^n = 1, B^2 = 1, BA = A^{-1}B \rangle$  has three basic relations. Let's examine their implications.

**$A^n = 1$ :** This means that any expression involving  $A$ 's and  $B$ 's need not have any string of successive  $A$ 's longer than  $n-1$ , because any block of  $n$  successive  $A$ 's is  $A^n$  which, because it is equal to the identity, can be removed.

For example in  $D_4 = \langle A, B \mid A^4 = 1, B^2 = 1, BA = A^{-1}B \rangle$ , an element such as  $AABAAAAAABA$  can be simplified to  $AABAAABA = A^2BA^3BA$  by removing an  $A^4$  from the middle.

**$B^2 = 1$ :** This means that it is never necessary to have two successive  $B$ 's. For example in  $D_8$  an expression such as  $ABBBAAABBAA$  can be simplified to  $ABAAAAA$  by using  $B^2 = 1$ , twice. This can be further reduced to  $ABA$  by use of the relation  $A^4 = 1$ .

Another consequence of  $B^2 = 1$  is  $B = B^{-1}$  (just multiply both sides on the left by  $B^{-1}$ ). This means that there is never any need to have  $B^{-1}$  in any expression.

**BA = A<sup>-1</sup>B:** It is this third relation that makes dihedral groups non-abelian (except for the trivial cases of D<sub>4</sub> and D<sub>2</sub> where A<sup>-1</sup> = A). Expressing this relation in words, we can say that every time a B passes across an A it inverts it, that is, converts it to A<sup>-1</sup>.

Consequently if we have an expression involving a mixture of A's and B's we can move all the A's up to the front and all the B's down to the back just as we would if the commutative law was in force. The difference is that the A's get inverted every time a B crosses over. This is the dihedral "twist".

**Example 13:** The expression ABA<sup>3</sup>BA<sup>2</sup>BAB can be written as:

$$AA^{-3}BBA^2BAB = A^{-2}BBA^2BAB = A^{-2}A^2BAB = BAB = A^{-1}B^2 = A^{-1}.$$

**Theorem 21:** The elements of D<sub>2n</sub> are:

$$\begin{aligned} &1, A, A^2, A^3, \dots, A^{n-1}, \\ &B, AB, A^2B, A^3B, \dots, A^{n-1}B \end{aligned}$$

**Proof:** Because of the relation BA = A<sup>-1</sup>B we can express every element in the form A<sup>i</sup>B<sup>j</sup>. But because A<sup>n</sup> = 1 and B<sup>2</sup> = 1, we may assume that i = 0, 1, 2, ... , n-1 and j = 0 or 1.

Notice that the first row consists of the cyclic subgroup, H, generated by A, and the second row is the left coset HB.

**Theorem 22:** In the dihedral group  $\langle A, B \mid A^n = 1, B^2 = 1, BA = A^{-1}B \rangle$  the elements of the form A<sup>k</sup>B all have order 2.

**Proof:** (A<sup>k</sup>B)<sup>2</sup> = A<sup>k</sup>BA<sup>k</sup>B = A<sup>k</sup>A<sup>-k</sup>BB = BB = 1.

## §4.10. Groups of Order 2p

We now classify groups of order 2p (where p is prime). We show that all such groups are either cyclic or dihedral. Since the proof is rather lengthy we have broken the argument up into 39 steps. Also, to make it easier to see which assumptions are in force at any given time, we've used a similar indenting convention to that advocated when writing computer programs.

**Theorem 23:** If  $|G| = 2p$  for some prime p then G is cyclic or dihedral.

**Proof:**

(1) Suppose that  $|G| = 2p$  where p is prime

(2) Suppose that p is odd.

(3) By Lagrange's theorem the order of every element is 1, 2, p or 2p.

(4) Suppose G contains an element of order 2p.

(4) Hence G is cyclic.

(5) Since  $|G|$  is even, G must contain an element, b, of order 2.

(6) Suppose that *all* the elements of G, except 1, have order 2.

(7) Then G is abelian.

(8) Choose a, b ∈ G of order 2 with a ≠ b.

(9) Hence H = {1, a, b, ab} is a subgroup of G of order 4.

(10) Since 4 does not divide 2p we get a contradiction.

(11) So G must have an element, a, of order p.

- (12) Let  $H = \langle a \rangle$ .
- (13) Since 2 does not divide  $p$ ,  $b \notin H$ .
- (14) The right cosets of  $H$  in  $G$  must be  $H$  and  $bH$ .
- (15) Similarly the left cosets are  $H$  and  $Hb$ .
- (16) Since  $bH$  and  $Hb$  consist of all the elements outside  $H$ , they must be equal, ie.  $Hb = bH$ .
- (17) Now  $ba \in bH$  so  $ba \in Hb$ .
- (18) Hence  $ba = a^r b$  for some integer  $r = 0, 1, \dots, p-1$ .
- (19) Hence  $b^2 a = ba^r b$
- (20)  $= baa \dots ab$  (where there are  $r$  factors of  $a$ ).
- (21)  $= a^r a^r \dots a^r b^2$  (where there are  $r$  factors of  $a^r$ ).
- (22)  $= a^{r^2}$  (since  $b^2 = 1$ ).
- (23) So  $a^{r^2} = a$ ,
- (24) Hence  $p$  divides  $r^2 - 1$ .
- (25) Since  $p$  is prime and  $r^2 - 1 = (r-1)(r+1)$ ,  $p \mid r-1$  or  $p \mid r+1$ .
- (26) Thus  $ba = ab$  or  $a^{-1}b$ .
- (27) Suppose  $ba = ab$ .
- (28) Now the order of  $ab$  must be 1, 2 or  $p$ .
- (29) Suppose  $ab = 1$ .
- (30) Then  $a = b^{-1} = b$ , a contradiction.
- (31) Suppose  $ab$  has order 2.
- (32) Then  $1 = (ab)^2 = a^2 b^2 = a^2$ , a contradiction.
- (33) Suppose  $ab$  has order  $p$ .
- (34) Then  $1 = (ab)^p = a^p b^p = b^p$ , a contradiction.
- (35) So  $b^{-1}ab = a^{-1}$  and so  $G = \langle a, b \mid a^p = b^2 = 1, ba = a^{-1}b \rangle = D_{2p}$ .
- (36) Suppose that  $p = 2$ .
- (37) Then every element of  $G$  (except 1) has order 2.
- (38) Hence  $G$  is abelian.
- (39) Hence  $G = \langle a, b \mid a^2 = b^2 = 1, ba = ab \rangle = \langle a, b \mid a^2 = b^2 = 1, ba = a^{-1}b \rangle = D_4$ .

## EXERCISES

**EXERCISE 1:** Show that the set of all matrices over  $\mathbf{Z}_2$  of the form  $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$  is a group of order 8 under matrix multiplication. Does it satisfy the commutative law?

**EXERCISE 2:** Find all the elements of order 4 in the above group.

**EXERCISE 3:** Show that the above group is a dihedral group of order 8, that is find an element  $A$  of order 4 and an element of order 2 such that  $BA = A^{-1}B$ .

**EXERCISE 4:** Find all the elements of order 4 in  $\mathbf{Z}_2 \oplus \mathbf{Z}_8$ .

**EXERCISE 5:** How many elements of the group  $C^\#$  of non-zero complex numbers under multiplication have order 7? How many have order 8?

**EXERCISE 6:** The following is a partially completed group table for a group. Complete it.

	a	b	c	d
a		a		
b			c	
c			a	
d		d		

Which element is the identity?

**EXERCISE 7:** Find all 4 possible group tables for a group  $G = \{1, a, b, c\}$  of order 4. Show that three of them are isomorphic (meaning that any one of them can be transformed to any other by a suitable relabelling) and the fourth is fundamentally different (eg look at the number of elements of order 2).

**EXERCISE 8:** If  $G$  is the group whose table is given below, show that  $H = \{1, c, d\}$  and  $K = \{1, b\}$  are both subgroups of  $G$ . Find all the left and right cosets of each subgroup.

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	1	c	b	e	d
b	b	d	1	e	a	c
c	c	e	a	d	1	b
d	d	b	e	1	c	a
e	e	c	d	a	b	1

**EXERCISE 9:**

If  $G = \langle a, b \mid a^4 = 1, b^3 = 1, ab = ba \rangle$  and  $H$  is the cyclic subgroup generated by  $b$ , find the right and left cosets of  $H$  in  $G$ .

**EXERCISE 10:** In the dihedral group  $D_{10} = \langle a, b \mid a^5 = 1, b^2 = 1, ab = ba^{-1} \rangle$ , simplify  $a^7 b^3 a^{-2} b a b a^3 b a^2 a^7 b^2 a$ .

**EXERCISE 11:** Simplify  $a^{13} b^5 a^2 b^{-7} a^2 b a$  in the above group  $D_{10}$ .

**EXERCISE 12:** Find the order of  $H$  given the following clues:

- (a)  $H$  is a proper subgroup of a group of order 68
- (b)  $H$  is non-cyclic

**EXERCISE 13:** Find the order of  $H$  given the following clues.

- (a)  $H$  is a subgroup of some group of order 100.
- (b)  $H$  contains no element of order 2.
- (c)  $H$  is not cyclic.

**EXERCISE 14:** Find the order of  $H$  given the following clues:

- (a)  $H$  is a subgroup of some group  $G$  of order 168.
- (b)  $H$  is a subgroup of another group  $K$  of order 112.
- (c)  $H$  is not cyclic or dihedral.
- (d)  $H$  contains an element of order 7.
- (e)  $H$  has more than two left cosets in  $K$ .

**EXERCISE 15:** If  $G$  is a group, the *centre* (*zentrum* in German) of  $G$  is defined to be  $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$ . In other words, it is the set of all elements that commute with everything.

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

(b) Find  $Z(D_{2n})$ . [HINT: You will need to consider odd and even values of  $n$  separately.]

**EXERCISE 16:** Let  $G = \{x \in \mathbb{R} \mid x \neq -1\}$  denote the set of real numbers excluding  $-1$ , and let the binary operation  $*$  be defined on  $G$  by  $a * b = a + b + ab$

(i) Prove that  $(G, *)$  is a group.

(ii) What is the inverse of  $2$ ?

(iii) How many elements does  $G$  have of order  $2$ ?

**EXERCISE 17:** Find the numbers of elements of each order in the following two groups whose group tables are given:

(a)

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

(b)

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

**EXERCISE 18:** Find the orders of the elements in the cyclic group of order  $6$ .

**EXERCISE 19:** Find the orders of the elements of the following three groups:

$G =$  the group  $\{0, 1, 2, 3, 4, 5, 6, 7\}$  under addition modulo  $8$ ;

$H =$  the group  $\{1, 3, 7, 9, 11, 13, 17, 19\}$  under multiplication modulo  $20$ ;

$K =$  the dihedral group of order  $8$ .

Show that no two of these groups are isomorphic.

**EXERCISE 20:** Which of the above three groups of order  $8$  is cyclic? Which are abelian?

**EXERCISE 21:** Find  $\langle 9 \rangle$ , the cyclic group generated by  $9$ , in the group  $\mathbb{Z}_{100}^\#$ . This consists of all the integers from  $1$  to  $99$  that have no factors in common with  $100$ . The operation is multiplication modulo  $100$ . Also determine the order of  $9$  in this group.

**EXERCISE 22:** Find the order of the following elements in the group  $\mathbb{Z}_{100}$  (consisting of all the integers from  $0$  to  $99$  under addition modulo  $100$ ):  $2, 9, 6, 15$ .

**EXERCISE 23:**

Find the left and right cosets of  $\{1, b\}$  in the dihedral group

$$D_{12} = \langle a, b \mid a^6 = 1, b^2 = 1, ab = ba^{-1} \rangle.$$

**EXERCISE 24:**  $G$  is the group whose table is given below. Show that  $H = \{1, a, d, f\}$  and  $K = \{1, d\}$  are both subgroups of  $G$ . Find all the left and right cosets of each subgroup.

	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	d	e	g	f	c	1	b
b	b	g	d	1	c	a	e	f
c	c	e	1	d	b	f	g	a
d	d	f	c	b	1	g	a	e
e	e	b	f	a	g	d	c	1
f	f	1	g	e	a	b	d	c
g	g	c	a	f	e	1	b	d

**EXERCISE 25:** Find the order of  $H$  given the following clues:

- $H$  is a proper subgroup of a group of order 52.
- $H$  is non-abelian.

**EXERCISE 26:** Find the order of  $H$  given the following clues:

- $H$  is a subgroup of some group  $G$  of order 100.
- $H$  is a subgroup of another group  $K$  of order 40.
- $H$  is not cyclic or dihedral.

**EXERCISE 27:** Find the order of  $H$  given the following clues:

- $H$  is a subgroup of some group  $G$  of order 20.
- $H$  is non-abelian.
- $G$  contains an element  $g$  of order 2 and an element  $h$  of order 5.
- $H$  contains  $h$  but not  $g$ .

**EXERCISE 28:** If  $G$  is a group, the *derived subgroup* of  $G$  is defined to be the subgroup generated by all the elements of the form  $x^{-1}y^{-1}xy$  as  $x, y$  range over the elements of the group. Find the derived subgroup of  $D_{2n}$ . [HINT: You will need to consider odd and even values of  $n$  separately.]

**EXERCISE 29:** Complete the following group table and find the orders of the elements.

	1	a	b	c	d	e
1						
a		1	c	b		d
b			d	a	1	
c		d	e		a	b
d		c		e	b	a
e		b	a		c	1

**EXERCISE 30:** Find the numbers of elements of each order in the cyclic group of order 12.

**EXERCISE 31:** Find the order of the following elements in the group  $\mathbf{Z}_{17}^\#$  (consisting of all the integers from 1 to 16 under multiplication modulo 17):  
2, 6, 9, 16

**EXERCISE 32:** Find the orders of the elements of the following three groups:

**G** = the group  $\{\pm 1, \pm i, \pm(1+i)/\sqrt{2}, \pm(1-i)/\sqrt{2}\}$  under multiplication;

**H** = the group of symmetries of a rectangular box;

**K** = the group of order 8 whose group table is:

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Show that no two of these groups are isomorphic.

## SOLUTIONS

**EXERCISE 1:**

There are  $2^3 = 8$  matrices of this form, over  $\mathbf{Z}_2$ . 
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$$
 so

the set is closed under matrix multiplication. The associative law holds, as it always does

with matrix multiplication. The identity matrix has this form. Finally the inverse of  $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$

is  $\begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$  which has the required form. Finally  $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$  while

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$  so the group does not satisfy the commutative law.

**EXERCISE 2:**

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

**EXERCISE 3:**

Take  $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$  and  $B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ .

**EXERCISE 4:**

The elements of  $\mathbf{Z}_2 \oplus \mathbf{Z}_8$  are vectors of the form  $(x, y)$  where  $x \in \mathbf{Z}_2$  and  $y \in \mathbf{Z}_8$ . If  $4(x, y) = (0, 0)$  then  $4x = 0$  and  $4y = 0$ . This places no restriction on  $x$ :  $x = 0$  or  $1$  but  $4y = 0$  means  $y = 0, 2, 4$  or  $6$ . If  $2(x, y) = (0, 0)$  then  $2y = 0$ . So we must exclude  $y = 0$  and  $y = 4$ . The elements of order 4 are thus  $(0, 2), (0, 6), (1, 2)$  and  $(1, 6)$ .

**EXERCISE 5:**

There are 6 elements of order 7, namely  $e^{\pi i/7}, \dots, e^{6\pi i/7}$  and 4 elements of order 8, namely  $e^{\pi i/8}, e^{3\pi i/8}, e^{5\pi i/8}, e^{7\pi i/8}$ .

**EXERCISE 6:**

Since  $bc = c$  the element  $b$  is the identity. So we can complete the corresponding row and column:

	a	b	c	d
a		a		
b	a	b	c	d
c		c	a	
d		d		

Now  $dc$  cannot be any of  $a, c$  or  $d$  because that would result in a repetition in either the row or the column corresponding to  $d$ . So  $dc$  must be  $b$ . In a similar way we can complete the table:

	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	a	b
d	c	d	b	a

**EXERCISE 7:**

Filling out the entries for the identity we get:

	1	a	b	c
1	1	a	b	c
a	a			
b	b			
c	c			

Now  $ab = 1$  or  $c$ .

Case I  $ab = 1$ : We can now complete the group table:

	1	a	b	c
1	1	a	b	c
a	a	c	1	b
b	b	1	c	a
c	c	b	a	1

Case II:  $ab = c$ : The group table is thus:

	1	a	b	c
1	1	a	b	c
a	a		c	
b	b			
c	c			

Now  $bc = 1$  or  $a$ .

Case IIA  $bc = 1$ : The group table is thus:

	1	a	b	c
1	1	a	b	c
a	a		c	
b	b	c	a	1
c	c		1	

If  $a^2 = b$  then  $ac = 1$ , a contradiction. Hence  $a^2 = 1$  and so the group table is:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	a	1
c	c	b	1	a

Case IIB  $bc = a$ : The group table is:

	1	a	b	c
1	1	a	b	c
a	a		c	
b	b	c	1	a
c	c		a	

This can be completed in two possible ways:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

Of these four possibilities the ones that arise in Cases I and IIA are isomorphic to the second possibility under Case IIB. They thus represent a single group with differing notation. This group has just one element of order 2. The remaining possibility (the first under Case IIB) is essentially different in that it has 3 elements of order 2. There are thus two groups of order 4. Note that both of them are abelian.

### EXERCISE 8:

The fact that H and K are subgroups of G can be most easily seen by extracting their group tables from the main table:

H	1	c	d
1	1	c	d
c	c	d	1
d	d	1	c

<b>K</b>	<b>1</b>	<b>b</b>
<b>1</b>	<b>1</b>	<b>b</b>
<b>b</b>	<b>b</b>	<b>1</b>

Since every entry in each table belongs to the subset in each case each subset is closed under multiplication. Clearly each contains the identity and, since 1 appears in each row and column, every element has an inverse within the respective subset.

The left cosets of H in G are:

$$H = \{1, c, d\} \text{ and}$$

$$aH = \{a1, ac, ad\} = \{a, b, e\}.$$

The right cosets of H in G are:

$$H = \{1, c, d\} \text{ and}$$

$$Ha = \{1a, ca, da\} = \{a, e, b\}.$$

NOTE that in this example the left and right cosets are the same, even though the group is non-abelian.

The left cosets of K in G are:

$$K = \{1, b\} \text{ and}$$

$$aK = \{a1, ab\} = \{a, c\} \text{ and}$$

$$dK = \{d1, db\} = \{d, e\}.$$

NOTE that we didn't waste our time with bK or cK because those elements were already included and we would have simply repeated the first two cosets.

For example  $bK = \{b1, bb\} = \{b, 1\} = \{1, b\}$ . So always use as a representative for a new coset, an element which has not yet been included.

The right cosets of K in G are:

$$K = \{1, b\} \text{ and}$$

$$Ka = \{1a, ba\} = \{a, d\} \text{ and}$$

$$Kc = \{1c, bc\} = \{c, e\}$$

NOTE that in this case the left cosets and the right cosets give two different subdivisions of the group. Thus K is not one of these normal subgroups.

### EXERCISE 9:

The elements are: 1, a, a<sup>2</sup>, a<sup>3</sup>,  
b, ab, a<sup>2</sup>b, a<sup>3</sup>b,  
b<sup>2</sup>, ab<sup>2</sup>, a<sup>2</sup>b<sup>2</sup>, a<sup>3</sup>b<sup>2</sup>.

The left cosets are  $H = \{1, b, b^2\}$   
 $aH = \{a, ab, ab^2\}$   
 $a^2H = \{a^2, a^2b, a^2b^2\}$   
and  $a^3H = \{a^3, a^3b, a^3b^2\}$

Of course since this group is abelian the left cosets are the same as the right cosets.

**EXERCISE 10:**

Using  $b^2 = 1$  this becomes:

$a^7ba^{-2}baba^3ba^2a^7a$ , and combining powers of  $a$  we get  $a^7ba^{-2}baba^3ba^{10}$ . Using  $a^5 = 1$  we get  $a^2ba^3baba^3b$ . Now we need to make use of the relation  $ab = ba^{-1}$ . Moving a  $b$  past an  $a$ , inverts it. Moving the second last  $b$  to the back we get  $a^2ba^3baa^{-3}b^2 = a^2ba^3ba^3$ . Moving the next  $b$  down gives  $a^2ba^3a^{-3}b = a^2bb = a^2$ .

**EXERCISE 11:**

The expression can be successively simplified as follows:

$$a^{13}b^5a^2b^{-7}a^2ba \rightarrow a^3ba^2ba^2ba$$

$$\rightarrow a^3ba^2ba^2a^{-1}b = a^3ba^2bab \rightarrow a^3ba^2a^{-1} = a^3ba \rightarrow a^2b.$$

**EXERCISE 12:**

By Lagrange's Theorem divides 68. Since  $H$  is not cyclic and groups of prime order are cyclic,  $|H|$  is not prime. Similarly it is not 1 (groups of order 1 contain just the identity and are cyclic). So we are looking for a divisor of 68 which is neither 1 nor prime. Since the prime factorisation of 68 is  $2^2 \cdot 17$ , the only possibilities are 4 and 68. However since  $H$  is a *proper* subgroup, this means it is not the whole of  $G$  and so 68 is ruled out. Thus, by a process of elimination,  $|H| = 4$ .

**EXERCISE 13:**

By Lagrange's Theorem  $|H|$  divides 100.  $H$  being non-cyclic rules out 1 and the primes 2 and 5, leaving 4, 5, 10, 20, 25, 50 and 100. Now groups of even order must contain an element of order 2. Since  $H$  does not, it must have odd order, leaving 25 as the only possibility.

**EXERCISE 14:**

By Lagrange's Theorem,  $|H|$  divides both  $168 = 8 \times 3 \times 7$  and  $112 = 16 \times 7$  and therefore must divide their greatest common divisor, which is 56. Since  $H$  contains an element of order 7,  $|H|$  must be divisible by 7. This limits the possibilities to 7, 14, 28 and 56. Now since  $H$  is neither cyclic nor dihedral,  $|H|$  cannot be prime or twice a prime [groups of order  $p$  are cyclic; groups of order  $2p$  are cyclic or dihedral]. This narrows down the possibilities to 28 and 56. Now if  $|H|$  was 56 there would be exactly 2 left cosets in  $K$  which has order 112. By clue (e) this is not so, and hence 56 is ruled out. Therefore  $|H|$  must be 28.

**EXERCISE 15:**

(a) This is easily verified. Note that  $gx = xg$  implies that  $xg^{-1} = g^{-1}x$ . (b)  $D_{2n} = \langle a, b \mid a^n=1, b^2=1, ab=ba^{-1} \rangle$ . If  $a^r \in Z(G)$  then  $a^r b = ba^r = a^{-r}b$ , so  $a^{2r} = 1$  which means that  $n \mid 2r$ . If  $n$  is odd this means  $n \mid r$  and so  $a^r = 1$ . If  $n$  is even  $a^r$  is 1 or  $a^{n/2}$ . Similarly one can check that no element of the form  $a^r b$  commutes with  $a$ . So  $Z(D_{2n}) = \{1\}$  if  $n$  is odd and  $\{1, a^{n/2}\}$  if  $n$  is even.

**EXERCISE 16:**

**Closure:** Let  $a, b \in G$ , so  $a \neq -1$  and  $b \neq -1$ . Suppose  $a * b = -1$ . Then  $a + b + ab = -1$  and so  $(a + 1)(b + 1) = 0$  which implies that  $a = -1$  or  $b = -1$ , a contradiction.

**Associativity:** Unlike the examples in exercise 1, this is a totally new operation that we have never encountered before. We must therefore carefully check the associative law.

$$\begin{aligned}
(a * b) * c &= (a * b) + c + (a * b) c \\
&= ab + a + b + c + (ab + a + b)c \\
&= a + b + c + ab + ac + bc + abc
\end{aligned}$$

Similarly  $a * (b * c)$  has the same value (we can actually see this by the symmetry of the expression).

**Identity:** An identity,  $e$ , would have to satisfy:  $e * x = x = x * e$  for all  $x \in G$ , that is,  $ex + e + x = x$ , or  $e(x + 1) = 0$  for all  $x$ . Clearly  $e = 0$  works. The identity is 0.

**Inverses:** If  $x * y = 0$ , then  $xy + x + y = 0$ . So  $y(x + 1) = -x$  and hence  $y = -x/(x + 1)$ . This exists for all  $x \neq -1$ , i.e. for all  $x \in G$ . But we must also check that it is itself an element of  $G$ . Suppose  $-x/(x + 1) = -1$ . Then  $-x = -x - 1$ , which gives  $0 = -1$ . This is clearly a contradiction and hence  $y$  must be in  $G$ .

### EXERCISE 17:

(a) has the 1 plus 3 elements of order 2.

(b) has 1, one element of order 2 (viz.  $b$ ) and 2 elements of order 4.

[The fact that they differ in their structure in this way means that they are non-isomorphic, or essentially different. These two tables reflect the only two possible group structures for a group of order 4.]

### EXERCISE 18:

The cyclic group of order 6 has the form:

$$\{1, g, g^2, g^3, g^4, g^5\} \text{ where } g^6 = 1$$

Clearly  $g$  has order 6.

$(g^2)^2 = g^4$ ,  $(g^2)^3 = g^6 = 1$  and so  $g^2$  has order 3.

$(g^3)^2 = 1$  and so  $g^3$  has order 2.

$(g^4)^2 = g^8 = g^2$ ,  $(g^4)^3 = g^{12} = 1$  and so  $g^4$  has order 3;

The powers of  $g^5$  are  $g^5$ ,  $g^{10} = g^4$ ,  $g^{15} = g^3 = g^{20} = g^2$ ,  $g^{25} = g$ . Finally  $(g^5)^6 = g^{30} = 1$  and so  $g^5$  has order 6.

The cyclic group of order 6 thus has:

1 element of order 1;

1 element of order 2;

2 elements of order 3;

2 elements of order 6.

NOTE: orders 4 and 5 are missed out. Can you guess why?

### EXERCISE 19:

**G:** 1, 3, 5, 7 have order 8

2, 6 have order 4

4 has order 2

0 has order 1

**H:** 3, 7, 13 and 17 have order 4

9, 11 and 19 have order 2

1 has order 1

**K:** The dihedral group

$\langle a, b \mid a^4 = b^2 = 1, ab = ba^{-1} \rangle$  has elements:

1,  $a$ ,  $a^2$ ,  $a^3$ ,  $b$ ,  $ab$ ,  $a^2b$ ,  $a^3b$ . Of these:

$a$ ,  $a^3$  have order 4

$a^2$ ,  $b$ ,  $ab$ ,  $a^2b$ ,  $ba^3$  have order 2;

1 has order 1.

NOTE: The order of the group is a power of 2 and the orders of the elements are likewise powers of 2. This is quite significant.

Listing the numbers of the elements of orders 1, 2, 4 and 8 as vectors we have:

G: (1,1,2,4); H: (1,3,4,0); K: (1,5,2,0)

The differences show that these three groups are mutually non-isomorphic. There are in fact 5 distinct groups of order 8, the above three plus two others.

**EXERCISE 20:**

G is cyclic (and hence abelian) because it contains an element of order 8; H is abelian but not cyclic; K is non-abelian (and hence not cyclic).

NOTE: There is always only one cyclic group of any given order. In other words, all cyclic groups of order n are isomorphic. A representative example of the cyclic group of order n is  $Z_n = \{0, 1, \dots, n-1\}$  of integers modulo n under addition.

**EXERCISE 21:**

The powers of 9 are:

$$9^1 = 9, 9^2 = 81$$

$9^3 = 729 = 29 \pmod{100}$  and so on. Rather than accumulate the higher and higher powers we can simply multiply by 9 at each stage to get the next:

$$9^4 = 9 \times 29 = 261 = 61$$

Then comes 49, 41, 69, 21, 89 and finally 1.

So  $\langle 9 \rangle = \{1, 9, 81, 29, 61, 49, 41, 69, 21, 89\}$ . There are 10 elements in this cyclic subgroup and so 9 has order 10 under multiplication modulo 100.

**EXERCISE 22:**

**2:** Remember that the operation is addition, so we need to keep adding the generator to itself, that is, taking higher and higher multiples, not powers. We want the smallest positive integer n such that  $2n = 0 \pmod{100}$ , or in other words, such that 2n is a multiple of 100. The answer is clearly 50.

**9:** We want 100 to divide 9n. Since 100 has no factors in common with 9, we would need n itself to be a multiple of 100. The smallest positive such n is thus 100. So 9 has order 100 in this group.

**6:** We need 6n to be a multiple of 100. Since 2 divides both 6 and 100 we need 50 to divide 3n. But since 50 has no factor in common with 3, we'd need 50 to divide n. So 6 has order 50.

**15:**  $15n = 0 \pmod{100}$  means  $3n = 0 \pmod{20}$ . Since 3 is coprime with 20, we need  $n = 0 \pmod{20}$ , so 15 has order 20.

**EXERCISE 23:**

Left cosets:

1	b	a	ab	a <sup>2</sup>	a <sup>2</sup> b	a <sup>3</sup>	a <sup>3</sup> b	a <sup>4</sup>	a <sup>4</sup> b	a <sup>5</sup>	a <sup>5</sup> b
---	---	---	----	----------------	------------------	----------------	------------------	----------------	------------------	----------------	------------------

Right cosets

1	b	a	ba	a <sup>2</sup>	ba <sup>2</sup>	a <sup>3</sup>	ba <sup>3</sup>	a <sup>4</sup>	ba <sup>4</sup>	a <sup>5</sup>	ba <sup>5</sup>
---	---	---	----	----------------	-----------------	----------------	-----------------	----------------	-----------------	----------------	-----------------

i.e.

1	b	a	a <sup>5</sup> b	a <sup>2</sup>	a <sup>4</sup> b	a <sup>3</sup>	a <sup>3</sup> b	a <sup>4</sup>	a <sup>2</sup> b	a <sup>5</sup>	ab
---	---	---	------------------	----------------	------------------	----------------	------------------	----------------	------------------	----------------	----

**EXERCISE 24:**

H and K contain 1 and are closed under multiplication and inverse as these tables show:

<b>H</b>	1	a	d	f
1	1	a	d	f
a	a	d	f	1
d	d	f	1	a
f	f	1	a	d

<b>K</b>	1	d
1	1	a
d	d	1

The left and right cosets of H are

1	a	d	f	b	c	e	g
---	---	---	---	---	---	---	---

The left and right cosets of K are

1	d	a	f	b	c	e	g
---	---	---	---	---	---	---	---

Both H and K are normal subgroups.

**EXERCISE 25:**

By (a)  $|H| = 1, 2, 4, 13, 26$  and by (b)  $|H| = 26$

**EXERCISE 26:**

By (a)  $|H|$  divides 100. By (b)  $|H|$  divides 40. Hence  $|H|$  divides  $100 - 80 = 20$ . Hence  $|H| = 1, 2, 4, 10$  or 20. By (c)  $|H| = 20$ .

**EXERCISE 27:**

By (a)  $|H|$  divides 20. By (c), (d)  $|H|$  is divisible by 5. Hence  $|H| = 5, 10$  or 20. By (b)  $|H| \neq 5$ . By (d)  $|H| \neq 20$ . Hence  $|H| = 10$ .

**EXERCISE 28:**

Let  $G = D_{2n} = \langle a, b \mid a^n = 1, b^2 = 1, ba = a^{-1}b \rangle$ . Since  $a^{-1}b^{-1}ab = a^{-2}$ ,  $a^2 \in G'$  and hence  $G'$  contains all even powers of  $a$ .

**Case I:  $n$  is even.** Let  $H = \langle a^2 \rangle$ . Since  $b^{-1}a^{2k}b = a^{-2k} \in H$ ,  $H$  is a normal subgroup of  $G$ . Since  $|G/H| = 4$ ,  $G/H$  is abelian and so  $G' \leq H$ . Thus  $G' = H = \langle a^2 \rangle$ .

**Case II:  $n$  is odd, say  $n = 2m + 1$ .** Let  $H = \langle a \rangle$ . Since the order of  $a$  is odd  $\langle a^2 \rangle = H$  (this is because  $a = a^{n-2m} = a^{-2m}$ ). Hence  $H \leq G'$ . But  $|G/H| = 2$  and so  $G/H$  is cyclic and hence abelian. Thus  $G' \leq H$ . Hence  $G' = H = \langle a \rangle$ .

**EXERCISE 29:**

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	1	c	b	e	d
b	b	e	d	a	1	c
c	c	d	e	1	a	b
d	d	c	1	e	b	a
e	e	b	a	d	c	1

**EXERCISE 30:**

If  $G = \langle a \mid a^{12} = 1 \rangle$  there are 4 elements of order 12 ( $a, a^5, a^7, a^{11}$ ), 2 elements of order 6 ( $a^2, a^{10}$ ), 2 elements of order 4 ( $a^3, a^9$ ), 2 elements of order 3 ( $a^4, a^8$ ), 1 element of order 2 ( $a^6$ ) plus the identity of order 1.

**EXERCISE 31:**

The group has order 16 so the possible orders of the elements are powers of 2.

**2:**  $2^2 = 4, 2^4 = 16 = -1, 2^8 = 1$  so 2 has order 8.

**6:**  $6^2 = 2$  so 6 has order 8.

**9:**  $9^2 = 13 = -4, 9^4 = 16 = -1, 9^8 = 1$  so 9 has order 4.

**15:**  $16^2 = (-1)^2 = 1$  so 16 has order 2.

**EXERCISE 32:**

$G$  is the group of 8<sup>th</sup> roots of 1. The four elements  $\pm(1+i)/\sqrt{2}, \pm(1-i)/\sqrt{2}$  have order 8,  $\pm i$  have order 4,  $-1$  has order 2 and 1 has order 1.

$H = \langle A, B, C \mid A^2 = B^2 = C^2 = 1, BA = AB, AC = CA, CB = BC \rangle$ . It has 7 elements of order 2 plus the identity.

$K$ : has 6 elements of order 4 ( $\pm i, \pm j, \pm k$ ), only 1 element of order 2 ( $-1$ ), plus the identity.

Since these three groups differ in the numbers of elements of each order no two of them can be isomorphic.

