These are all different, since if $g_i g_r = g_i g_s$ then the left cancellation rule implies that $g_r = g_s$. Similarly, the right cancellation rule implies that the [illegible] column of the group table are all different. In other words

a group table is a latin square.

The simplest example of a latin square of order m is the grou[illegible] $\mathbb{Z}_m$ with respect to the + operation. We now know that *any* fi[illegible] a latin square, but as we might expect, not every latin square [illegible] some group (see Ex. 20.3.5).

Theorem 20.3.2 If a and b are any elements of a group [illegible]

$$ax = b$$

has a unique solution in G.

Proof If x and $\bar{x}$ are both solutions of the equation, then

$$ax = a\bar{x} \quad (= b),$$

and so, by the left cancellation rule, $x = \bar{x}$. Hence there is at most one solution. Clearly $x = a^{-1}b$ is a solution, since

$$a(a^{-1}b) = (aa^{-1})b = 1b = b,$$

and so there is exactly one solution. □

In the case $a = b$ the theorem implies that there is a unique solution of the equation $ax = a$. Since any identity element of G satisfies this equation we conclude that

G has a unique identity element.

Similarly, in the case $b = 1$ the theorem implies that there is a unique solution of the equation $ax = 1$. Since any inverse of a satisfies this equation, we conclude that

each element of G has a unique inverse.

As a consequence of these observations we are justified in speaking of *the* identity element of G and *the* inverse of a in G.

Exercises 20.3

1 Show that the inverse of ab is $b^{-1}a^{-1}$.

2 Establish the following implications, where x and y are any elements of a group:

(i) $xy = 1 \quad \Rightarrow yx = 1$;

(ii) $(xy)^2 = x^2y^2 \Rightarrow xy = yx$.

(In part (ii) x^2 stands for xx.)

3 Suppose that G is a group with the property that $g^2 = 1$ for all g in G. Prove that G is a commutative group.

Proof If s is a multiple of m, say $s = mk$, then

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

where we use the rules for manipulating powers and the fact th
Conversely, suppose $x^s = 1$. By Theorem 8.2 we can write

$$s = mq + r, \qquad 0 \le r < m.$$

Then

$$1 = x^s = x^{mq+r} = (x^m)^q x^r = x^r$$

since $x^m = 1$. Now if $r > 0$ the equation $x^r = 1$ contradicts the definition of m as the least positive integer for which $x^m = 1$. Consequently, we must have $r = 0$ and $s = mq$, so s is a multiple of m, as required. □

Exercises 20.4

1 Let α and β denote the permutations of $\mathbb{N}_7$ whose representations in cycle notation are

$$\alpha = (15)(27436), \qquad \beta = (1372)(46)(5).$$

Calculate the orders of α and β, considered as elements of the symmetric group S_7. What are the orders of $\alpha\beta$ and $\beta\alpha$?

2 Let x and y be elements of a finite group G. Show that the orders of x and yxy^{-1} are the same.

3 Let M denote the set of matrices of the form

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

where the entries are members of $\mathbb{Z}_7$ and $a \neq 0$. Show that M is a group with respect to matrix multiplication, and find the orders of the elements

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}.$$

4 Let G be the group defined as in Ex. 3, except that the entries of the matrices are now real numbers rather than elements of $\mathbb{Z}_7$. Show that G contains infinitely many elements of order 2.

5 Let u and v be elements of a commutative group, and suppose that their orders are r and s, respectively. Show that if r and s are distinct primes then the order of uv is rs.

20.5 Isomorphism of groups

Recall the two examples considered in Section 20.2. In *Example 1* we discussed the group $G_\triangle$ whose elements are the six symmetries of an equilateral triangle, $G_\triangle = \{i, r, s, x, y, z\}$. In *Example 2* we discussed another group G_M which turns out to have six elements; they are the matrices which we shall denote by

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad R = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix},$$

$$X = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \quad Y = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}, \quad Z = \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix},$$

where the symbols 0, 1, and 2 are elements of $\mathbb{Z}_3$. For the moment let us forget the definitions of $G_\triangle$ and G_M and concentrate on their group tables (Tables 20.5.1a,b).

Table 20.5.1(a)

	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	y	z	x
s	s	i	r	z	x	y
x	x	z	y	i	s	r
y	y	x	z	r	i	s
z	z	y	x	s	r	i

Table 20.5.1(b)

	I	R	S	X	Y	Z
I	I	R	S	X	Y	Z
R	R	S	I	Y	Z	X
S	S	I	R	Z	X	Y
X	X	Z	Y	I	S	R
Y	Y	X	Z	R	I	S
Z	Z	Y	X	S	R	I

Clearly, the group tables are essentially the same—the notation has been carefully chosen to emphasize this. Thus, insofar as group properties are concerned, $G_\triangle$ and G_M are identical; they differ only in the names given to their elements. More formally, we have a bijection $\beta\colon G_\triangle \to G_M$ which takes i to I, r to R, and so on, and which preserves the group operation. For example, $rx = y$ in $G_\triangle$ and $RX = Y$ in G_M, which implies that

$$\beta(rx) = \beta(y) = Y = RX = \beta(r)\beta(x).$$

Definition If G_1 and G_2 are groups (both written in the multiplicative notation), then a bijection $\beta\colon G_1 \to G_2$ is said to be an **isomorphism** if, for all g and g' in G_1

$$\beta(gg') = \beta(g)\beta(g').$$

When there is such an isomorphism, G_1 and G_2 are said to be **isomorphic**, and we write $G_1 \approx G_2$.

Exercises 20.5

1 Describe the four symmetries of a rectangle, and construct the group table. By writing down a suitable bijection show that your group is isomorphic to the one whose group table is Table 20.5.2.

Table 20.5.2

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

2 By analysing the possible group tables show that, if isomorphic groups are regarded as the same, then

(i) there is just one group of order 2;

(ii) there is just one group of order 3;

(iii) there are just two groups of order 4.

3 Show that the isomorphism relation $\approx$ is an equivalence relation.

4 Suppose that G_1 and G_2 are finite groups and $\beta\colon G_1 \to G_2$ is an isomorphism. If $x_2 = \beta(x_1)$ for a given element x_1 in G_1, prove that x_1 and x_2 have the same order.

Thus there is no element of order 8 in $C_2 \times C_4$ and [illegible] $C_2 \times C_4$ cannot be isomorphic to C_8. □

The fact that $C_2 \times C_3 \approx C_6$ is a special case of the following theorem.

Theorem 20.6 If m and n are coprime positive integers then

$$C_m \times C_n \approx C_{mn}.$$

Proof Suppose C_m, C_n are generated by x, y, respectively, and let z denote the element (x, y) of $C_m \times C_n$. Let r be the order of z in $C_m \times C_n$. We shall show that $r = mn$.

Since $z^r = (x^r, y^r)$, and the identity of $C_m \times C_n$ is $(1, 1)$, the equation $z^r = 1$ implies that $x^r = 1$ in C_m and $y^r = 1$ in C_n. Consequently, by Theorem 20.4, r is a multiple of m and a multiple of n. Since r is the least positive integer for which $z^r = 1$, it must be the *least* common multiple of m and n. Hence, by Ex. 8.7.8,

$$r = \operatorname{lcm}(m, n) = \frac{mn}{\gcd(m, n)} = mn,$$

since m and n are coprime.

Since $C_m \times C_n$ has mn elements, and it contains an element z of order mn, it must be a cyclic group. □

Exercises 20.6

1 Let U be the subset of $\mathbb{Z}_7$ which contains all the elements of $\mathbb{Z}_7$ except 0. Show that multiplication in $\mathbb{Z}_7$ defines a group operation for U, and that $U \approx C_6$.

2 Let M denote the set of 2×2 matrices of the form

$$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix},$$

where the entries are integers. Show that M, with respect to matrix multiplication, is an infinite cyclic group.

3 Write out the details of the proof that the direct product $A \times B$ of two groups is a group.

4 Show that the two distinct groups of order 4 which you obtained in Ex. 20.5.2 are isomorphic to C_4 and $C_2 \times C_2$.

20.7 Subgroups

A subset H of a group G is said to be a **subgroup** of G if the members of H form a group with respect to the group operation in G.

Example 1 Let $G_\triangle = \{i, r, s, x, y, z\}$ be the group of symmetries of the triangle, as in *Example 1*, Section 20.2. Which of the following subsets of $G_\triangle$ are subgroups?

$$H_1 = \{r, s, z\}, \quad H_2 = \{i, r, s\}, \quad H_3 = \{i, r, s, x\}.$$

Example 2 Given any group G, let $Z(G)$ denote th[illegible] of those elements which commute with every element of G, th[illegible]

$$Z(G) = \{z \in G \mid zg = gz \text{ for al[illegible]}$$

Show that $Z(G)$ is a subgroup of G (it is called the [illegible]

Solution We verify tine conditions **S1** and **S2**. Suppose x and y are in $Z(G)$, so that $xg = gx$ and $yg = gy$ for all g in G. We have

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

so that xy is in $Z(G)$, and **S1** is verified. Also, on multiplying the equation $xg = gx$ by x^{-1} on both sides we obtain

$$x^{-1}(xg)x^{-1} = x^{-1}(gx)x^{-1},$$

and using the associative law we obtain $gx^{-1} = x^{-1}g$. Thus x^{-1} is in $Z(G)$ and **S2** is verified. □

If x is an element of order m in a group G then the elements

$$1, x, x^2, \ldots, x^{m-1}$$

of G form the **cyclic subgroup** $\langle x \rangle$ generated by x. It is very easy to verify that $\langle x \rangle$ is indeed a subgroup (Ex. 20.7.6), and clearly

the order of x is equal to the order of the subgroup $\langle x \rangle$.

For example, let U be the group of non-zero elements of $\mathbb{Z}_7$, with respect to multiplication (Ex. 20.6.1). On computing the powers of 2 in U we find

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1,$$

so 2 has order 3 and the cyclic subgroup $\langle 2 \rangle$ contains the three elements 1, 2, 4. On the other hand, the cyclic subgroup $\langle 3 \rangle$ is the whole of U since

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

Exercises 20.7

1 Which of the following are subgroups of $G_\triangle$?

$$K_1 = \{i, x\}, \qquad K_2 = \{i, x, y\}, \qquad K_3 = \{i, r, s, x, y\}.$$

2 Use the group $G_\triangle$ to provide an example of the fact that if H and K are subgroups then $H \cup K$ need not be a subgroup.

3 Show that if H and K are subgroups of G then so is $H \cap K$.

4 Let g be a given element of a group G and let $C(g)$ denote the set of elements of G which commute with g, that is

$$C(g) = \{x \in G \mid xg = gx\}.$$

Show that $C(g)$ is a subgroup of G. What is the relationship between these subgroups and the centre $Z(G)$?

5 If G is the group of the square (Ex. 20.2.2), find $C(g)$ for each g in G, and then find $Z(G)$.

6 Use Theorem 20.7 to verify that if x is an element of order m in a group G then $\langle x \rangle = \{1, x, \ldots, x^{m-1}\}$ is a subgroup of G.