

Lecturer: Dr Stephen Glasby

### Tutorial and Assignment

1. Let  $\iota$  denote the identity map  $X \rightarrow X: x \mapsto x$ .

(i) If  $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$  is the injective function defined by

$$f(1) = b, f(2) = c, \text{ and } f(3) = d,$$

then find three functions  $g: \{a, b, c, d\} \rightarrow \{1, 2, 3\}$  such that  $g \circ f = \iota$ .

(ii) If  $f: \{1, 2, 3, 4\} \rightarrow \{a, b, c\}$  is the surjective function defined by  $f(1) = b, f(2) = c, f(3) = a$  and  $f(4) = b$ , then find two functions  $g: \{a, b, c\} \rightarrow \{1, 2, 3, 4\}$  such that  $f \circ g = \iota$ .

*Solution.*

You should draw a picture for these questions.

(i)  $g(a)$  can be any of 1, 2 or 3,  $g(b) = 1$ ,  $g(c) = 2$ ,  $g(d) = 3$ .

(ii)  $g(a) = 3$ ,  $g(b)$  is 1 or 4,  $g(c) = 2$ .

2. Let  $\iota_X$  denote the identity map  $X \rightarrow X: x \mapsto x$ , and let  $f$  be a map  $X \rightarrow Y$ .

(i) Show that  $f$  is injective iff there exists a function  $g: Y \rightarrow X$  such that  $g \circ f = \iota_X$ .

(ii) Show that  $f$  is surjective iff there exists a function  $g: Y \rightarrow X$  such that  $f \circ g = \iota_Y$ .

(iii) Show that  $f$  is bijective iff  $f$  is invertible.

*Solution.*

(i) If  $g \circ f = \iota_X$  and  $f(x_1) = f(x_2)$ , then

$$\begin{aligned} x_1 &= \iota_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) \\ &= g(f(x_2)) = (g \circ f)(x_2) = \iota_X(x_2) = x_2. \end{aligned}$$

(Let me explain what I mean by the phrase “well-defined”. Recall that a function can only map an element to one other element. If  $y = f(x_1) = f(x_2)$ , then according to our definition of  $g$ ,  $g(y) = x_1$  and  $g(y) = x_2$ . This is OK since  $x_1 = x_2$ .) Furthermore,  $g(f(x)) = x$  so  $g \circ f = \iota_X$ .

- (ii) Suppose that  $f \circ g = \iota_Y$  and  $y \in Y$ . Then  $f(g(y)) = y$  so  $f(x) = y$  where  $x = g(y)$ . Hence  $f$  is surjective. Conversely, suppose that  $f$  is surjective. Define  $g: Y \rightarrow X$  by  $g(y) = x$  where  $x$  is one of the elements satisfying  $f(x) = y$ . Then  $f(g(y)) = f(x) = y$  so  $f \circ g = \iota_Y$ .
- (iii) This follows from (i) and (ii) as  $f$  is invertible if there exists a function  $g$  satisfying  $g \circ f = \iota_X$  and  $f \circ g = \iota_Y$ .

**3.** Prove that an identity element in a group is unique.

*Solution.*

Let  $e$  and  $e'$  be two identity elements. Then  $xe = ex = x$  and  $e'x = xe' = x$ . Hence  $ee' = e'$  since  $e$  is an identity and  $ee' = e$  since  $e'$  is an identity.

**4.** Prove that every element of a group has a unique inverse.

*Solution.*

Let  $y$  and  $y'$  be two inverses of  $x$ . Then  $xy = yx = e$  and  $xy' = y'x = e$ . Hence

$$y = ye = y(xy') = (yx)y' = ey' = y'.$$

**5.** Use the associative law to prove that

$$(a(bc))d = ((ab)c)d = (ab)(cd) = a(b(cd)) = a((bc)d).$$

*Solution.*

Since  $a(bc) = (ab)c$  it follows that  $(a(bc))d = ((ab)c)d$ , and since  $b(cd) = (bc)d$  it follows that  $a(b(cd)) = a((bc)d)$ . If  $x = ab$ , then  $(xc)d = x(cd)$  so  $((ab)c)d = (ab)(cd)$ , and similarly if  $y = cd$ , then  $a(by) = (ab)y$  so  $a(b(cd)) = (ab)(cd)$ .

*Solution.*

There is no ambiguity if  $n = 1$  or  $n = 2$ . Suppose now that  $n \geq 3$  and that the value of the product  $b_1 \cdots b_r$ ,  $1 \leq r < n$ , is independent of the bracketing used. Consider the two bracketings  $(a_1 \cdots a_r)(a_{r+1} \cdots a_n)$  and  $(a_1 \cdots a_s)(a_{s+1} \cdots a_n)$  where by induction, the bracketing inside the brackets does not matter. If  $r = s$ , these products are clearly equal. If  $r \neq s$  assume without loss of generality that  $r < s$ . It follows from the associative law that

$$\begin{aligned}(a_1 \cdots a_r)(a_{r+1} \cdots a_n) &= (a_1 \cdots a_r)[(a_{r+1} \cdots a_s)(a_{s+1} \cdots a_n)] \\ &= [(a_1 \cdots a_r)(a_{r+1} \cdots a_s)](a_{s+1} \cdots a_n) \\ &= (a_1 \cdots a_s)(a_{s+1} \cdots a_n).\end{aligned}$$

This completes the inductive proof.

\*7. The purpose of this exercise is to show that parts of the group axioms are consequences of others and so do not need to be verified when showing an object is a group. Let  $G$  be a set with a binary operation which satisfies:

- (1)  $x(yz) = (xy)z$  for all  $x, y, z \in G$ ,
- (2) there exists an  $e \in G$  such that  $xe = x$  for all  $x \in G$ , and
- (3) for all  $x \in G$  there exists a  $y \in G$  such that  $xy = e$ .

- (i) Show the right cancellation law holds.
- (ii) Show that  $(ex)y = xy$  and deduce that  $ex = x$ .
- (iii) Show that  $yx = e$ .
- (iv) Deduce that  $G$  is a group.

*Solution.*

- (i) Suppose that  $ax \stackrel{(4)}{=} bx$  and  $xy = e$ . Then

$$a \stackrel{(2)}{=} ae \stackrel{(3)}{=} a(xy) \stackrel{(1)}{=} (ax)y \stackrel{(4)}{=} (bx)y \stackrel{(1)}{=} b(xy) \stackrel{(3)}{=} be \stackrel{(2)}{=} b.$$

- (ii) Now  $(ex)y \stackrel{(1)}{=} e(xy) \stackrel{(3)}{=} ee \stackrel{(2)}{=} e$  and  $xy = e$ . It follows from  $(ex)y = xy$  and the right cancellation law that  $ex = x$ .
- (iii) Now  $ey \stackrel{(ii)}{=} ye \stackrel{(3)}{=} y(xy) \stackrel{(1)}{=} (yx)y$ . Using (i) it follows that  $yx = e$ .
- (iv) From (ii) and (iii), it follows that  $G$  is a group.

- (i) If  $S$  is a finite set containing an identity element  $e$ , and the map  $S \rightarrow S: x \mapsto xy$  is injective for every  $y$  in  $S$ , show that each  $y \in S$  has a (left) inverse.
- (ii) If  $p$  is a prime, deduce that the set

$$\mathbb{Z}_p^\times = \{a + p\mathbb{Z} \mid a = 1, 2, \dots, p-1\}$$

is a group under multiplication.

*Solution.*

- (i) Given  $y \in S$  there is an  $x \in S$  (by the pigeon-hole principle) such that  $xy = e$ .
- (ii) Suppose that  $a + p\mathbb{Z}$  and  $b + p\mathbb{Z}$  are not equal to  $0 + p\mathbb{Z}$ . Then

$$(a + p\mathbb{Z})(b + p\mathbb{Z}) = ab + p\mathbb{Z} \neq 0 + p\mathbb{Z}.$$

(Otherwise  $p$  divides  $ab$ , and since  $p$  is a prime,  $p$  divides  $a$  or  $b$  contrary to the fact that  $a + p\mathbb{Z}$  and  $b + p\mathbb{Z}$  are not equal to  $0 + p\mathbb{Z}$ .) If  $b + p\mathbb{Z} \neq 0 + p\mathbb{Z}$ , then it follows that the map  $a + p\mathbb{Z} \mapsto ab + p\mathbb{Z}$  is injective (why?). Hence it follows from (i) that inverses exist in  $\mathbb{Z}_p^\times$ . (In general, it is useful to use Euclid's algorithm to find inverses.) The associative law clearly holds, and  $1 + p\mathbb{Z}$  is the identity element. Hence  $\mathbb{Z}_p^\times$  is a group.

- 9.** (i) Prove that addition modulo  $n$  is well-defined. That is, if  $a_1 + n\mathbb{Z} = a_2 + n\mathbb{Z}$  and  $b_1 + n\mathbb{Z} = b_2 + n\mathbb{Z}$ , then prove that  $(a_1 + n\mathbb{Z}) + (b_1 + n\mathbb{Z}) = (a_2 + n\mathbb{Z}) + (b_2 + n\mathbb{Z})$ .
- (ii) Prove that addition modulo  $n$  is associative.

*Solution.*

- (i) Note that  $a_1 + n\mathbb{Z} = a_2 + n\mathbb{Z}$  if and only if  $a_1 - a_2 \in n\mathbb{Z}$ . Hence in this part we know that  $a_1 - a_2 \in n\mathbb{Z}$  and  $b_1 - b_2 \in n\mathbb{Z}$  and want to show that  $(a_1 + a_2) - (b_1 + b_2) \in n\mathbb{Z}$ . Since  $n\mathbb{Z}$  is closed under addition, it follows that  $(a_1 - a_2) + (b_1 - b_2) \in n\mathbb{Z}$  and so the result follows.
- (ii) Since  $a + (b + c) = (a + b) + c$  in  $\mathbb{Z}$ , it follows that

$$a + (b + c) + n\mathbb{Z} = (a + b) + c + n\mathbb{Z}.$$

(ii) Prove that multiplication modulo  $n$  is associative.

*Solution.*

(i) Suppose that  $a_1 = a_2 + \alpha n$  and  $b_1 = b_2 + \beta n$ . Then

$$\begin{aligned}(a_1 + n\mathbb{Z})(b_1 + n\mathbb{Z}) &= a_1 b_1 + n\mathbb{Z} \\ &= (a_2 + \alpha n)(b_2 + \beta n) + n\mathbb{Z} \\ &= a_2 b_2 + (a_2 \beta + \alpha b_2 + \alpha \beta n)n + n\mathbb{Z} \\ &= a_2 b_2 + n\mathbb{Z} \\ &= (a_2 + n\mathbb{Z})(b_2 + n\mathbb{Z}).\end{aligned}$$

(ii) Since  $a(bc) = (ab)c$  in  $\mathbb{Z}$ , it follows that

$$a(bc) + n\mathbb{Z} = (ab)c + n\mathbb{Z}.$$

11. Which of the following sets form a group under multiplication modulo 20 ?

(i)  $\{1, 3, 7, 9\}$

(ii)  $\{1, 9, 13, 17\}$

(iii)  $\{1, 10\}$

(iv)  $\{0, 5, 10\}$

*Solution.*

In parts (i), (ii) and (iii) the identity element is clearly the number 1. By exercise 10 the associative law holds, so we need only check whether the product of elements in  $S$  is in  $S$  (i.e. whether  $S$  is closed under multiplication), and whether inverses exist. One way to see that  $S$  is a group is to draw the multiplication table for  $S$ . If  $S$  is closed then all the entries will be from  $S$ . If each element has an inverse, then each row and column contains the identity element. Note that if the same entry appears in a row or column, then it follows from the cancellation law that  $S$  is not a group. (In this example, the multiplication table will be symmetric (why?). Can you use the pigeon-hole principle to show that if  $S$  is a group, then every row or column of the multiplication table is a rearrangement of  $S$ ?) To briefly indicate which of the laws of closure, associativity, identity, inverses I will use a string. For example TTFF means that the first two laws hold but the last two do not.

(i) Every product of  $\{1, 3, 7, 9\}$  is determined by the table

1	3	7	9
3	9	1	7
7	1	9	3
9	7	3	1

(ii) Every product of  $\{1, 9, 13, 17\}$  is determined by the table

1	13	17	9
13	9	1	17
17	1	9	13
9	17	13	1

Hence  $S$  is a group. A quicker proof that  $S$  is a group is to note that  $1 = 13^0, 13 = 13^1, 9 = 13^2, 17 = 13^3, 1 = 13^4$ . Can we say that this group and the previous group are “structurally identical”? (TTTT)

(iii) Not a group as  $10 \times 10 = 0$  so multiplication is not closed. (FTTF)

(iv) The cancellation law does not hold as  $5 \times 0 = 0 \times 0$  does not imply that  $5 = 0$ . (TTTF, note that 5 is the identity element.)

**12.** Which of the following sets form a group under multiplication modulo 14? (State which group properties do not hold.)

(i)  $\{0, 7\}$

(ii)  $\{1, 3, 5\}$

(iii)  $\{1, 9, 11\}$

(iv)  $\{1, 7, 13\}$

*Solution.*

(i) The cancellation law does not hold as  $7 \times 0 = 0 \times 0$  does not imply that  $7 = 0$ . (TTTF)

(ii) Not a group as  $3 \times 3 = 9 \notin S$ . (FTTT)

(iii) Note that  $1 = 9^0, 9 = 9^1, 11 = 9^2, 1 = 9^3$  so  $S$  is a (cyclic) group with 3 elements. (TTTT)

(iv) The cancellation law does not hold as  $7 \times 1 = 7 \times 7$  does not imply that  $1 = 7$ . (TTTF)

**13.** Decide which of the following systems are groups. Among the groups, which are abelian?

(i)  $G = \mathbb{Z}$ , the set of integers, under subtraction.

(ii)  $G = \{0\}$  under multiplication.

(iii)  $G = \mathbb{Z}^{>0}$ , the natural numbers under multiplication.

(v)  $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{R}, a \neq 0 \right\}$  under matrix multiplication.

(vi)  $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, ac \neq 0 \right\}$  under matrix multiplication.

*Solution.*

(i) Not a group as the associative law fails e.g.  $(3 - 2) - 1 \neq 3 - (2 - 1)$ . Indeed,  $(a - b) - c \neq a - (b - c)$  whenever  $c \neq 0$ . (TFFF)

(ii)  $G$  is an abelian group. (TTTT)

(iii)  $G$  is not a group as 2 has no inverse. Note that  $2x \neq 1$  for all  $x \in \mathbb{Z}$ . Note that multiplication is closed, the associative law holds and 1 is the identity element. (TTTF)

(iv)  $G$  is an abelian group. Suppose  $\frac{a_i}{b_i} \in G$  where  $a_i, b_i \in \mathbb{Z}$ ,  $i = 1, 2$ , and the  $b_i$  are odd integers. Then

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

is an element of  $G$  since  $b_1 b_2$  is an odd integer and  $a_1 b_2 + a_2 b_1 \in \mathbb{Z}$ .  $0 = \frac{0}{1}$  is the identity,  $-\frac{a}{b} = \frac{-a}{b}$  and the commutative law holds. (TTTT)

(v)  $G$  is an abelian group. Note that closure holds since

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} aa' & ab' + ba' \\ 0 & aa' \end{pmatrix} \in G.$$

Furthermore it follows from the above equation that multiplication is commutative. The associative law holds for matrices. The identity element is in  $G$ : set  $a = 1$  and  $b = 0$ , and  $G$  is closed under inverses since

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \frac{1}{a^2} \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} \in G.$$

(vi)  $G$  is a group which is not abelian. Note that closure holds since

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & ac' \end{pmatrix} \in G.$$

Furthermore multiplication is not commutative since

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \text{ and}$$

$a = 1, b = 0$  and  $c = 1$ , and  $G$  is closed under inverses since

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} \in G.$$

(TTTT)

14. Prove that there is only one group of order 3 by constructing its multiplication table.

*Solution.*

Let  $\{1, x, y\}$  be the elements of the group. The multiplication table must be

$$\begin{array}{ccc} 1 & x & y \\ x & y & 1 \\ y & 1 & x \end{array}$$

Note that  $xx = x$  violates the cancellation law. Now  $xx = 1$  implies  $xy = y$ , otherwise there will be two different elements in the same row of the table. But  $xy = y$  and  $1y = y$  violate the cancellation law. Hence we can not have  $xx = x$  or  $xx = 1$  and so must have  $xx = y$ . The rest of the table is now easy to complete.

15. If  $G$  is a multiplicative group such that  $(xy)^2 = x^2y^2$  for all  $x, y \in G$ , prove that  $G$  is abelian.

*Solution.*

We want to show that  $yx = xy$  for all  $x, y \in G$ . This follows from the equation  $xyxy = xxyy$  by cancelling  $x$  on the left and cancelling  $y$  on the right.

- \*16. If  $G$  is a finite group, show that

$$|G| - |\{x \in G \mid x^2 = e\}|$$

is an even number.

*Solution.*

Let  $S$  be the set  $\{x \in G \mid x^2 = e\}$ . If  $y \notin S$ , then  $y$  has odd order and so  $y^{-1} \notin S$  and  $y \neq y^{-1}$ . Therefore the elements in  $G$  but not in  $S$  are partitioned into pairs  $\{y, y^{-1}\}$ . Hence  $|G| - |\{x \in G \mid x^2 = e\}| = 2m$  where  $m$  is the number of pairs.

It suffices to describe the order of  $x^r$ ,  $r = 0, 1, \dots, 11$ , as  $x^{q^{12+r}} = x^r$ . These orders are 1, 12, 6, 4, 3, 12, 2, 12, 3, 4, 6 and 12 respectively.

18. (i) Find the order of each element of  $\mathbb{Z}_{12}$ .  
(ii) Find the elements of  $\mathbb{Z}_{12}^\times$ . (Any conjectures?)

*Solution.*

- (i) This question is the same as exercise 17 except that the notation now is additive rather than multiplicative. Thus we have

$x$	0	1	2	3	4	5	6	7	8	9	10	11
$ x $	1	12	6	4	3	12	2	12	3	4	6	12

- (ii)  $\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$ . In general  $\mathbb{Z}_n^\times$  consists of the elements of  $a + n\mathbb{Z}$  with  $\gcd(a, n) = 1$ , these elements have inverses and also have (additive) order  $n$ .
- \*19. The greatest common divisor of two integers  $m$  and  $n$  is denoted by  $\gcd(m, n)$  and satisfies  $\{xm + yn \mid x, y \in \mathbb{Z}\} = \gcd(m, n)\mathbb{Z}$ .
- (i) Show that  $d = \gcd(m, n)$  is indeed the greatest common divisor by proving:  
(a)  $d|m$  and  $d|n$ , and (b) if  $d'|m$  and  $d'|n$ , then  $d'|d$ . (Note that (a) shows that  $d$  is a common divisor, and (b) shows that every other common divisor divides  $d$ .)
- \*(ii) If  $x$  has order  $n$ , and  $\gcd(m, n) = 1$ , show that  $x^m$  also has order  $n$ .
- \*(iii) If  $x$  has order  $n$  show that  $x^m$  has order  $n/\gcd(m, n)$ .

*Solution.*

- (i) By definition,  $d$  divides every element of  $d\mathbb{Z} = \{xm + yn \mid x, y \in \mathbb{Z}\}$ . Hence  $d|m$  (put  $x = 1$  and  $y = 0$ ) and  $d|n$  (put  $x = 0$  and  $y = 1$ ). If  $d'|m$  and  $d'|n$ , then  $d'|(xm + yn)$  for every  $x, y \in \mathbb{Z}$ . But there are values of  $x$  and  $y$  for which  $xm + yn = d$ , so  $d'|d$ .
- (ii) Now  $(x^m)^n = (x^n)^m = e^m = e$ . Suppose that  $(x^m)^k = e$ . Then  $x^{mk} = e$  and by a theorem in lectures,  $n|mk$ . Since  $\gcd(m, n) = 1$ , it follows that  $n|k$ . Therefore,  $n$  is the smallest positive integer such that  $(x^m)^n = e$ , and so is, by definition, the order of  $x^m$ .



$$(i) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 2 & 9 & 1 & 6 & 5 & 8 & 4 \end{pmatrix},$$

$$(ii) \quad (1, 2, 3, 4)(5, 6)(7, 8, 9)$$

*Solution.*

(i) The inverse is

$$\begin{pmatrix} 7 & 3 & 2 & 9 & 1 & 6 & 5 & 8 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}.$$

As there is a convention to write the first line in ascending order, we write

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 2 & 9 & 7 & 6 & 1 & 8 & 4 \end{pmatrix}.$$

$$(ii) \quad (9, 8, 7)(6, 5)(4, 3, 2, 1) = (1, 4, 3, 2)(5, 6)(7, 9, 8).$$

**23.** Compute the product  $xy$  (where, as usual, composition is from right-to-left).

(i)

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 2 & 9 & 1 & 6 & 5 & 8 & 4 \end{pmatrix}$$

$$y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 3 & 7 & 2 & 8 & 4 & 6 & 9 \end{pmatrix},$$

$$(ii) \quad x = (1, 2, 3, 4)(5, 6)(7, 8, 9) \quad y = (1, 3, 5, 7, 9)(2, 4, 6, 8),$$

$$(iii) \quad x = (1, 2, 3, 4)(5, 6)(7, 8, 9) \quad y = (2, 4),$$

$$(iv) \quad x = (1, 2, 3, 4)(5, 6)(7, 8, 9) \quad y = (2, 5),$$

*Solution.*

$$(i) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 7 & 2 & 5 & 3 & 8 & 9 & 6 & 4 \end{pmatrix},$$

$$(ii) \quad (1, 4, 5, 8, 3, 6, 9, 2),$$

$$(iii) \quad (1, 2)(3, 4)(5, 6)(7, 8, 9), \quad (iv) \quad (1, 2, 6, 5, 3, 4)(7, 8, 9).$$

Parts (iii) and (iv) are part of a general pattern. If  $x$  is a permutation which is the product of  $r$  disjoint cycles and  $y$  is a transposition  $(a, b)$ , then  $xy$  is a

then the above fact may be used to prove that  $\text{sign}(g)\text{sign}(h) = \text{sign}(gh)$ .

**24.** Express the following permutations as a product of disjoint cycles

$$(i) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \qquad (ii) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

$$(iii) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 2 & 6 & 5 & 4 & 3 \end{pmatrix} \qquad (iv) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 4 & 6 & 5 & 7 \end{pmatrix}$$

*Solution.*

$$(i) \quad (1, 6)(2, 5)(3, 4) \qquad (ii) \quad (1, 2, 3, 4, 5, 6)$$

$$(iii) \quad (2, 7, 3)(4, 6) \qquad (iv) \quad (1, 3, 2)(5, 6)$$

**25.** Express the following permutations as a product of disjoint cycles

$$(i) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} \qquad (ii) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

$$(iii) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 2 & 4 & 3 & 6 & 1 \end{pmatrix} \qquad (iv) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 1 & 2 & 7 & 6 \end{pmatrix}$$

*Solution.*

$$(i) \quad (1, 3, 5)(2, 4, 6) \qquad (ii) \quad (1, 4)(2, 5)(3, 6)$$

$$(iii) \quad (1, 7)(2, 5, 3) \qquad (iv) \quad (1, 3, 5, 2, 4)(6, 7)$$

**26.** Determine the parity of the following permutations. (That is, which are even and which are odd.)

$$(1, 2, 3, 4, 5), (1, 5, 8, 6, 3, 7), (1, 2, 3, 4)(5, 6, 7, 8), (1, 2, 3, \dots, 2n).$$

*Solution.*

$$\begin{aligned} (1, 2, 3, 4, 5) &= (1, 5)(1, 4)(1, 3)(1, 2) \\ (2, 5, 7, 6, 3) &= (2, 3)(2, 6)(2, 7)(2, 5) \\ (1, 2, 3, 4)(5, 6, 7, 8) &= (1, 4)(1, 3)(1, 2)(5, 8)(5, 7)(5, 6) \text{ and} \\ (1, 2, 3, \dots, 2n) &= (1, 2n) \dots (1, 3)(1, 2). \end{aligned}$$

**27.** Determine the parity of the following permutations. Is there a quick way to determine the parity of a permutation?

$$(3, 4, 5, 6, 7, 8), (1, 8, 3, 6)(2, 7, 9)(4, 5), (1, 2, 3, \dots, 2n + 1).$$

*Solution.*

Since

$$(3, 4, 5, 6, 7, 8) = (3, 4)(4, 5)(5, 6)(6, 7)(7, 8)$$

and

$$(1, 8, 3, 6)(2, 7, 9)(4, 5) = (1, 8)(8, 3)(3, 6)(2, 7)(7, 9)(2, 5)$$

are a product of 5 and 6 transpositions respectively, these permutations are respectively odd and even. Now  $(1, 2, 3, \dots, 2n + 1) = (1, 2n + 1) \dots (1, 3)(1, 2)$  is even as it is a product of an even number of cycles, and by exercise 26 a cycle of even length is a product of an odd number of transpositions. Hence the parity of a permutation which is the product of (not necessarily disjoint) cycles, is even if it has an even number of cycles of even length, and odd if it has an odd number of cycles of even length.

**28.** Let  $H$  be a subgroup of the group  $G$ . Show that

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

is a subgroup of  $G$ .

*Solution.*

Now  $gHg^{-1}$  is nonempty as  $e = geg^{-1} \in gHg^{-1}$ . If  $h_1, h_2 \in H$ , then

$$(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in gHg^{-1}$$

so  $gHg^{-1}$  is closed under products. Similarly,  $gHg^{-1}$  is closed under inverses as  $(gh_1g^{-1})^{-1} = gh_1^{-1}g^{-1} \in gHg^{-1}$ . Hence  $gHg^{-1}$  is a subgroup of  $G$ . Note it is somewhat quicker to simultaneously note that  $gHg^{-1}$  is closed under products and inverses by noting that

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}.$$

The subgroup  $gHg^{-1}$  is called the *conjugate* of  $H$  by  $g$ .

Clearly  $e \in H$  and  $e \in K$  so  $e \in H \cap K$ . Let  $a, b \in H \cap K$ . It suffices to show that  $ab^{-1} \in H \cap K$ . Now  $a, b \in H$  and  $a, b \in K$  and  $H$  and  $K$  are subgroups so  $ab^{-1} \in H$  and  $ab^{-1} \in K$ . Hence  $ab^{-1} \in H \cap K$  as desired.

- \*30.** Let  $G = \langle x \rangle$  be a cyclic group and let  $H$  be a subgroup of  $G$ . Show that  $H$  is also cyclic.

*Solution.*

The proof of this exercise is similar to the proof of the fact that the only subgroups of  $\mathbb{Z}$  have the form  $n\mathbb{Z}$  for some  $n \in \mathbb{Z}$ . The difference here, is that the elements  $x^i, i \in \mathbb{Z}$ , of  $G$  need not all be distinct. That is, we could have  $x^i = x^j$  with  $i \neq j$ . As we shall see this complication does not hinder our original proof.

If  $H = \{e\}$ , then  $H = \langle e \rangle$  is cyclic. Suppose now that  $H$  is not the trivial subgroup. Let  $n$  be the smallest positive integer such that  $x^n$  is a nontrivial element of  $H$ . If  $x^m \in H$ , then write  $m = qn + r$  where  $0 \leq r < n$ . Since  $x^r = x^{m-qn} = x^m(x^n)^{-q} \in H$ , it follows by the usual argument that  $r = 0$  and  $H = \langle x^n \rangle$ .

- \*31.** Show that the order of an element of  $S_n$  is the least common multiple of the lengths of its disjoint cycles.

*Solution.*

Let  $g \in S_n$  have disjoint cycle decomposition  $c_1 c_2 \cdots c_r$ . Since the cycles are disjoint,  $c_i$  commutes with  $c_j$  (why?). Hence  $g^n = c_1^n c_2^n \cdots c_r^n$  and  $g^n = \iota$  if and only if  $c_i^n = \iota$  for each  $i$ . If  $c_i$  has length  $l_i, 1 \leq i \leq r$ , then  $c_i$  has order  $l_i$ , and the smallest value of  $n$  such that  $c_i^n = \iota$  for  $1 \leq i \leq r$ , is the least common multiple of the  $l_i$ . (The last step uses the fact that if  $|x| = l$  and  $x^m$  is the identity element, then  $l|m$ .)

- \*32.** Let  $G = \langle x \rangle$  be a cyclic group of finite order  $n$  and let  $m$  be a divisor of  $n$ . Show that  $G$  has a unique subgroup of order  $m$ .

*Solution.*

Suppose that  $n = qm$ . Then  $\langle x^q \rangle$  is a subgroup of order  $m$  (why?). Furthermore, it is the only such subgroup (why?).

- (i) transpositions,
- (ii) the transpositions  $(1, a), 1 < a \leq n$ ,
- \*(iii) the transpositions  $(a - 1, a), 1 < a \leq n$ .

*Solution.*

As the answers to these questions are not unique, your solution may differ from the ones below. Of course, you can always check your answer by multiplying the permutations together. The three basic principles underlying the three parts are:

$$\begin{aligned}
 (a_1, a_2, a_3, \dots, a_r) &= (a_1, a_2)(a_2, a_3) \cdots (a_{r-1}, a_r) \\
 (a, b) &= (1, a)(1, b)(1, a) \quad \text{if } 1 \notin \{a, b\} \\
 (c, d) &= (c, c+1, c+2, \dots, d)(c, c+1, \dots, d-1)^{-1} \quad \text{if } c < d \\
 &= (c, c+1)(c+2, c+3) \cdots (d-1, d) \\
 &\quad (d-2, d-1) \cdots (c, c+1)
 \end{aligned}$$

$$\begin{aligned}
 (1, 2, 3, 4) &= (1, 2)(2, 3)(3, 4) \\
 &= (1, 4)(1, 3)(1, 2) \\
 &= (1, 2)(2, 3)(3, 4) \\
 (1, 3, 4)(2, 5) &= (1, 3)(3, 4)(2, 5) \\
 &= (1, 3)(1, 3)(1, 2)(1, 5)(1, 2) \\
 &= (1, 2)(2, 3)(1, 2)(3, 4)(2, 3)(3, 4)(4, 5)(3, 4)(2, 3) \\
 (2, 8, 3, 5)(4, 6, 7) &= (2, 8)(8, 3)(3, 5)(4, 6)(6, 7) \\
 &= (1, 2)(1, 5)(1, 3)(1, 8)(1, 2)(1, 4)(1, 7)(1, 6)(1, 4) \\
 &= (2, 3)(3, 4)(4, 5)(3, 4)(2, 3)(3, 4)(4, 5)(5, 6)(6, 7) \\
 &\quad (7, 8)(6, 7)(5, 6)(4, 5)(3, 4)(2, 3)
 \end{aligned}$$

**34.** Express the permutations  $(2, 5), (1, 3, 4, 5, 2), (1, 3, 4, 5)(2, 4)$  as a product of:

- (i) transpositions,
- (ii) the transpositions  $(1, a), 1 < a \leq n$ ,
- \*(iii) the transpositions  $(a - 1, a), 1 < a \leq n$ .

$$\begin{aligned}
(2, 5) &= (2, 5) \\
&= (1, 2)(1, 5)(1, 2) = (1, 5)(1, 2)(1, 5) \\
&= (2, 3)(3, 4)(4, 5)(3, 4)(2, 3) \\
(1, 3, 4, 5, 2) &= (1, 3)(3, 4)(4, 5)(5, 2) \\
&= (1, 2)(1, 5)(1, 4)(1, 3) \\
&= (1, 2)(2, 3)(1, 2)(3, 4)(4, 5)(2, 3)(3, 4)(4, 5)(3, 4)(2, 3) \\
(1, 3, 4, 5)(2, 4) &= (1, 3)(3, 4)(4, 5)(2, 4) \\
&= (1, 5)(1, 4)(1, 3)(1, 2)(1, 4)(1, 2) \\
&= (1, 2)(2, 3)(1, 2)(3, 4)(4, 5)(3, 4)(2, 3)(3, 4)
\end{aligned}$$

**35.** For each  $g \in S_4$  below compute  $g(P)$  and  $\text{sign}(g)$  where  $P$  equals

$$\begin{aligned}
&(x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \\
&\quad (x_2 - x_3)(x_2 - x_4) \\
&\quad\quad (x_3 - x_4)
\end{aligned}$$

(i)  $g = (1, 2, 3, 4)$

(ii)  $g = (1, 2)(3, 4)$

(iii)  $g = (2, 3)$

*Solution.*

The respective values of  $g(P)$  are shown below. Hence the respective values of  $\text{sign}(g)$  are  $(-1)^4$ ,  $(-1)^2$  and  $(-1)^1$ .

(i)

$$\begin{aligned}
&(x_2 - x_3)(x_2 - x_4)(x_2 - x_1) \\
&\quad (x_3 - x_4)(x_3 - x_1) \\
&\quad\quad (x_4 - x_1)
\end{aligned}$$

(ii)

$$\begin{aligned}
&(x_2 - x_1)(x_2 - x_4)(x_2 - x_3) \\
&\quad (x_1 - x_4)(x_1 - x_3) \\
&\quad\quad (x_4 - x_3)
\end{aligned}$$

$$(x_3 - x_2)(x_3 - x_4) \\ (x_2 - x_4)$$

**36.** For each  $g \in S_5$  below compute  $g(P)$  and  $\text{sign}(g)$  where

$$P = \prod_{1 \leq i < j \leq 5} (x_i - x_j)$$

(i)  $g = (1, 2, 3, 4, 5)$

(ii)  $g = (1, 2)(3, 4)$

(iii)  $g = (3, 4)$

*Solution.*

The respective values of  $g(P)$  are shown below. Hence the respective values of  $\text{sign}(g)$  are  $(-1)^4$ ,  $(-1)^2$  and  $(-1)^1$ .

(i)

$$(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_2 - x_1) \\ (x_3 - x_4)(x_3 - x_5)(x_3 - x_1) \\ (x_4 - x_5)(x_4 - x_1) \\ (x_5 - x_1)$$

(ii)

$$(x_2 - x_1)(x_2 - x_4)(x_2 - x_3)(x_2 - x_5) \\ (x_1 - x_4)(x_1 - x_3)(x_1 - x_5) \\ (x_4 - x_3)(x_4 - x_5) \\ (x_3 - x_5)$$

(iii)

$$(x_1 - x_2)(x_1 - x_4)(x_1 - x_3)(x_1 - x_5) \\ (x_2 - x_4)(x_2 - x_3)(x_2 - x_5) \\ (x_4 - x_3)(x_4 - x_5) \\ (x_3 - x_5)$$

- (i)  $x = (1, 2)(3, 4), \quad y = (1, 3)(2, 4),$   
(ii)  $x = (1, 3, 5, 7, 9), \quad y = (1, 2, 3, 4)(5, 6).$

*Solution.*

Take care to conjugate  $y$  by  $x$  and not the other way around.

- (i)  $(6, 4, 1)(2, 3, 5) = (1, 6, 4)(2, 3, 5).$   
(ii)  $(2, 4)(1, 3) = (1, 3)(2, 4).$  That is,  $x$  centralizes  $y$ .  
(iii)  $(3, 2, 5, 4)(7, 6) = (2, 5, 4, 3)(6, 7).$

**38.** Use the substitution rule to compute  $xyx^{-1}$ , where

- (i)  $x = (1, 2, 3)(4, 5), \quad y = (1, 2, 3, 4, 5, 6),$   
(ii)  $x = (1, 2, 3)(4, 5, 6), \quad y = (1, 4)(2, 5)(3, 6),$   
(iii)  $x = (1, 3, 5, 7, 9), \quad y = (1, 7, 9, 2, 3, 4)(5, 6).$

*Solution.*

Take care to conjugate  $y$  by  $x$  and not the other way around.

- (i)  $(2, 3, 1, 5, 4, 6) = (1, 5, 4, 6, 2, 3).$   
(ii)  $(2, 5)(3, 6)(1, 4) = (1, 4)(2, 5)(3, 6).$   
If  $xyx^{-1} = y$ , we say that  $x$  *centralizes*  $y$ .  
(iii)  $(3, 9, 1, 2, 5, 4)(7, 6) = (1, 2, 5, 4, 3, 9)(6, 7).$

**39.** Use the substitution rule in reverse to find  $x$ , when possible, so that  $xyx^{-1} = z$ , where

- (i)  $y = (1, 3, 5, 7)(2, 4, 6)(8, 9), \quad z = (1, 2)(3, 4, 5, 6)(7, 8, 9),$   
(ii)  $y = (1, 2, 3)(4, 5), \quad z = (1, 2)(3, 4, 5),$   
(iii)  $y = (1, 2, 3, 4), \quad z = (1, 2)(3, 4),$   
(iv)  $y = (1, 3)(1, 2), \quad z = (1, 3, 2).$

then you are correct if and only if  $x_1x_2^{-1}$  centralizes  $y$ . Why is this so?) Remember both  $y$  and  $z$  must be written as a product of *disjoint* cycles, and to find  $x$  you may need to permute the orbits of  $z$  so that their lengths correspond to those of the orbits of  $y$ .

(i)

$$\begin{aligned} x &= \begin{pmatrix} 1 & 3 & 5 & 7 & 2 & 4 & 6 & 8 & 9 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 8 & 5 & 9 & 6 & 1 & 2 \end{pmatrix} \\ &= (1, 3, 4, 8)(2, 7, 6, 9) \end{aligned}$$

(ii)

$$\begin{aligned} x &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \\ &= (1, 3, 5, 2, 4) \end{aligned}$$

(iii) No solution for  $x$ , as  $y$  and  $z$  have different disjoint cycle types.

(iv) Note that  $y = (1, 2, 3)$  is its *disjoint* cycle decomposition. Hence

$$x = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3).$$

**40.** Use the substitution rule in reverse to find  $x$ , when possible, so that  $xyx^{-1} = z$ , where

$$(i) \quad y = (1, 4)(2, 3, 5, 6), \quad z = (1, 3, 5, 2)(4, 6),$$

$$(ii) \quad y = (1, 4)(2, 3, 5, 6), \quad z = (1, 3, 5, 2)(1, 6),$$

$$(iii) \quad y = (1, 2, 3)(4, 5, 6), \quad z = (1, 2)(3, 4)(5, 6),$$

$$(iv) \quad y = (1, 2, 3)(4, 5, 6), \quad z = (1, 3, 5)(2, 4, 6).$$

*Solution.*

$$(i) \quad x = \begin{pmatrix} 1 & 4 & 2 & 3 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix} = (1, 4, 6, 2)$$

(ii)  $y = (1, 4)(2, 3, 5, 6)$  and  $z = (1, 6, 3, 5, 2)$  have different *disjoint* cycle types and hence are not conjugate.

$$(ii) \quad x = (1 \ 3 \ 5 \ 2 \ 4 \ 6) = (2, 5, 6, 1)$$

**41.** Why does the substitution rule, for computing conjugates of permutations, work?

*Solution.*

If  $g(x) = y$ , we must show that  $(hgh^{-1})(h(x)) = h(y)$ . This is obvious since

$$(hgh^{-1})(h(x)) = h(g(h^{-1}h(x))) = h(g(x)) = h(y).$$

**\*42.** How many permutations in  $S_6$  have disjoint cycle structure

$$(i) \quad (a, b, c)(d, e)(f) ? \qquad (ii) \quad (a, b, c)(d, e, f) ?$$

*Solution.*

$$(i) \quad \frac{6 \cdot 5 \cdot 4}{3} \frac{3 \cdot 2}{2} \frac{1}{1} = 120$$

$$(ii) \quad \frac{1}{2!} \frac{6 \cdot 5 \cdot 4}{3} \frac{3 \cdot 2 \cdot 1}{3} = 40$$

**\*43.** How many permutations in  $S_6$  have disjoint cycle structure

$$(i) \quad (a, b)(c, d)(e, f) ? \qquad (ii) \quad (a, b, c, d, e, f) ?$$

*Solution.*

(i)  $\frac{1}{3!} \frac{6 \cdot 5}{2} \frac{4 \cdot 3}{2} \frac{2 \cdot 1}{2} = 15$ . Alternatively, you may assume that the permutation is in standard form  $(a, b)(c, d)(e, f)$ . The number of choices for  $a, b, c, d, e, f$  are 1, 5, 1, 3, 1, 1 respectively. These choices are independent so there are 15 possibilities.

(ii)  $\frac{6!}{6} = 5! = 120$ . Similarly, if  $(a, b, c, d, e, f)$  is in standard form, the number of choices for  $a, b, c, d, e, f$  are 1, 5, 4, 3, 2. So there are 5! such permutations.

*Solution.*

(i)

$$\iota, (a, b), (a, b, c), (a, b, c, d), (a, b, c, d, e), (a, b, c, d, e, f), \\ (a, b)(c, d), (a, b, c)(d, e), (a, b, c, d)(e, f), (a, b, c)(d, e, f), (a, b)(c, d)(e, f).$$

(ii) The largest order is 12 and this is obtained by elements of the form

$$(a, b, c, d)(e, f, g).$$

**45.** Show that  $xyx^{-1}y^{-1} = 1$  holds in a group if and only if  $xy = yx$ .

*Solution.*

Now  $xy = yx$  iff  $y^{-1}xy = x$  iff  $x^{-1}y^{-1}xy = e$ .

**\*46.** The sequence  $h = U^2R_M^2U^2R_M^2$  of moves of Rubik's cube swaps two pairs of edge "cubies" and fixes all the others. Numbering the cubies in some order, we can identify  $h$  with the permutation  $(1, 2)(3, 4)$ . Using  $h$ , or otherwise, find a sequence of moves which flips cubies 1 and 2 and fixes all remaining cubies. (A cubie is said to be *fixed* if it not moved, and an edge cubie is said to be *flipped* if the stays in the same "cubicle" but its orientation is reversed, so cubies and cubicles are to the cube what children and chairs are to the game of musical chairs.) Hint: Find a sequence of moves  $g$  that flips 1 and fixes 2,3,4 and possibly moves the other cubies.

*Solution.*

Now  $ghg^{-1}h$  is such a move. Since  $h = h^{-1}$ , this move can be written  $ghg^{-1}h^{-1}$ . We call  $ghg^{-1}h^{-1}$  a *commutator*, and it measures in some sense how close  $g$  and  $h$  are to commuting. One possibility for  $g$  is

$$g = D^{-1}R^{-1}D_M^{-1}R^{-1}D,$$

where as usual, composition is from right-to-left.

Alternatively, the sequence

$$f = R_M D^2 R_M^{-1} D^{-1} R_M D R_M^{-1}$$

The commutator  $U^{-1}f^{-1}Uf$  has a similar effect except it flips the upper front and upper right cubies. This last move, with appropriate reorientations of the cube, generates all possible edge-pair flips.

- \*47. Is there a sequence of moves of Rubik's cube which flips one edge cubie and fixes all other cubies?

*Solution.*

The moves of Rubik's cube induce many different permutations. For example, there are 9 squares on each of its 6 faces. A sequence of moves of the cube may therefore be identified with an element of the symmetric group  $S_{54}$ . For this problem, it is convenient to consider the moves of the cube as permuting a different set. Each move permutes the 12 edge cubies. Since each edge cubie has 2 squares on it, we are led to consider a subgroup of  $S_{24}$  (which is related to, but is different from, the subgroup of  $S_{54}$ ). The move in question corresponds to a transposition in  $S_{24}$ . However, the generating moves (i.e.  $L, R, U, D, F, B$ ) correspond to a product of two 4-cycles in  $S_{24}$  and hence are even permutations. There can be no product of these even permutations which equals the odd permutation in question. Can you see why we did not consider the subgroup of  $S_{54}$ ?

- \*48. Unscramble the edge cubies of a scrambled Rubik's cube. Can you devise an algorithm which will unscramble the edge cubies of a typical scrambled Rubik's cube? (Hint: Try using conjugates  $(ghg^{-1})$  and commutators  $(ghg^{-1}h^{-1})$  involving the move  $h = U^2R_M^2U^2R_M^2$ .)

*Solution.*

There are many solutions to this problem. Two good books, written by group theorists, on the subject of solving the cube are:

D.E. Taylor, *Mastering Rubik's Cube*, Book Marketing Australia Ltd, 1980.

D.E. Taylor and L. Rylands, *Cube Games*, Greenhouse Publications, Victoria, Australia, 1981.

The sequence

$$g = R_M D^{-1} R_M^{-1} D^{-1} F_M^{-1} D F_M D^{-1} R_M D R_M^{-1}$$

exchanges the upper front and upper right cubies while fixing the rest of the upper layer and preserving the upper face. Hence the commutator,  $U^{-1}g^{-1}Ug$  gives the cycle

(upper front, upper back, upper right)

correct cubicle. If some of the edge cubies need to be flipped, then the move in exercise 47 will complete our unscrambling of the edge cubies.

**49.** The *centralizer* of  $y \in G$  is defined to be

$$C_G(y) = \{ x \in G \mid xyx^{-1} = y \}.$$

If  $G = S_4$ , then compute  $C_G(y)$  by writing  $y$  in every possible way as a product of disjoint cycles, where

$$(i) \quad y = (1, 2, 3), \qquad (ii) \quad y = (1, 2)(3, 4).$$

*Solution.*

We use the substitution rule to find  $x$  such that  $xyx^{-1} = y'$  where  $y'$  is the same permutation as  $y$  but with a different disjoint cycle representation. We list all the possibilities for  $y'$  and the corresponding possibilities for  $x$ . The elements of  $C_{S_4}(y)$  are precisely these  $x$ .

(i) The possibilities for  $y'$  are  $(1, 2, 3)(4)$ ,  $(2, 3, 1)(4)$ ,  $(3, 1, 2)(4)$ . The corresponding  $x$  are  $\iota$ ,  $(1, 2, 3)$ ,  $(1, 3, 2)$ .

(ii) Now  $y'$  is one of

$$(1, 2)(3, 4), (1, 2)(4, 3), (2, 1)(3, 4), (2, 1)(4, 3), \\ (3, 4)(1, 2), (3, 4)(2, 1), (4, 3)(1, 2), (4, 3)(2, 1).$$

The corresponding  $x$  are

$$\iota, (3, 4), (1, 2), (1, 2)(3, 4), \\ (1, 3)(2, 4), (1, 3, 2, 4), (1, 4, 2, 3), (1, 4)(2, 3).$$

**50.** Which of the following subsets of  $X \times X$  are equivalence relations?

$$(i) \quad X = \mathbb{Q}, \{(x, y) \mid x - y \in \mathbb{Z}\}, \quad (ii) \quad X = \mathbb{R}, \{(x, y) \mid x - y \in \mathbb{Q}\},$$

$$(iii) \quad X = \mathbb{R}, \{(x, y) \mid x + y \in \mathbb{Q}\}, \quad (iv) \quad X = \mathbb{Z}, \{(x, y) \mid x - y \geq 0\},$$

$$(v) \quad X = \mathbb{R}^\times, \{(x, y) \mid x/y \in \mathbb{Q}^\times\}.$$

does not hold and the transitive axiom holds.

- (i) TTT equivalence classes:  $\{a + \mathbf{Z} \mid a \in \mathbb{R}\}$ . Indeed, we may assume that  $0 \leq a < 1$ .
- (ii) TTT equivalence classes:  $\{a + \mathbf{Q} \mid a \in \mathbb{R}\}$ .
- (iii) FTF  $(\sqrt{2}, \sqrt{2}) \notin S$ ;  $(\sqrt{2}, -\sqrt{2})$  and  $(-\sqrt{2}, \sqrt{2}) \in S$  but  $(\sqrt{2}, \sqrt{2}) \notin S$ .
- (iv) TFT  $(1, 0) \in S$  but  $(0, 1) \notin S$ .
- (v) TTT equivalence classes:  $\{a\mathbf{Q}^\times \mid a \in \mathbb{R}^\times\}$ .

**51.** What is wrong with the following argument which shows that the reflexive axiom for an equivalence relation is redundant? Let  $\sim$  be an equivalence relation on  $X$ . Given  $x \in X$ , choose  $y \in X$  such that  $x \sim y$ . Then  $y \sim x$  by symmetry and so by transitivity,  $x \sim x$ .

*Solution.*

There may not be any  $y$  such that  $x \sim y$ .

**52.** Let  $X$  be a subset of the group  $G$ , and let  $H$  be the set of all possible products of elements of  $X$  and their inverses. (The identity element is, by definition, the product of zero elements of  $X$ .)

- (i) Show that  $H$  is a subgroup of  $G$ .
- (ii) Show that  $H$  is the intersection of all subgroups of  $G$  that contain  $X$ . (In other words,  $H = \langle X \rangle$ .)

*Solution.*

- (i) What are the elements of  $H$ ? If  $X = \{x_1, x_2\}$ , then  $H$  equals

$$\begin{aligned} & \{e, x_1, x_2, x_1^{-1}, x_2^{-1}, \\ & x_1x_1, x_1x_2, x_1x_1^{-1}, x_1x_2^{-1}, \\ & x_2x_1, x_2x_2, x_2x_1^{-1}, x_2x_2^{-1}, \\ & x_1^{-1}x_1, x_1^{-1}x_2, x_1^{-1}x_1^{-1}, x_1^{-1}x_2^{-1}, \\ & x_2^{-1}x_1, x_2^{-1}x_2, x_2^{-1}x_1^{-1}, x_2^{-1}x_2^{-1}, \dots\}. \end{aligned}$$

words.) Clearly  $H$  is nonempty and if  $a, b$  are elements of  $H$ , i.e. words in  $X \cup X^{-1}$ , then  $ab^{-1}$  is also a word in  $X \cup X^{-1}$ . Hence  $ab^{-1} \in H$  and  $H$  is a subgroup of  $G$ .

- (ii) By (i),  $H$  is a subgroup of  $G$  containing the set  $X$ . Since  $\langle X \rangle$  is the intersection of all subgroups of  $G$  containing  $X$ , we have  $\langle X \rangle \subseteq H$ . Conversely, every subgroup containing  $X$  is closed under products and inverses and so contains  $H$ . Hence  $H \subseteq \langle X \rangle$  and equality follows.

**\*53.** Determine generators for the centralizers  $C = C_G(y)$  where

- (i)  $G = S_4$  and  $y = (1, 2, 3, 4)$ ,      (ii)  $G = S_n$  and  $y = (1, 2, \dots, n)$ ,  
 (iii)  $G = S_6$  and  $y = (1, 2, 3)(4, 5, 6)$   
 (iv)  $G = S_9$  and  $y = (1, 2, 3)(4, 5, 6)(7, 8, 9)$ .

*Solution.*

- (i)  $C = \langle (1, 2, 3, 4) \rangle$  (see (ii))  
 (ii) There are  $n$  ways to write  $y$  as a cycle namely

$$(1, 2, \dots, n-1, n), (2, 3, \dots, n, 1), \dots, (n, 1, \dots, n-2, n-1),$$

or in general as  $y' = (i, i+1, \dots, n, 1, \dots, i-1)$ . The substitution rule may be used in reverse to find  $x$  such that  $xyx^{-1} = y'$ . Note that

$$x = \begin{pmatrix} 1 & 2 & \dots & n-i+1 & n-i+2 & \dots & n \\ i & i+1 & \dots & n & 1 & \dots & i-1 \end{pmatrix} = y^i.$$

Hence  $C = \langle y \rangle$ .

- (iii) In this case the disjoint factors are either both fixed or are swapped. The element  $(1, 4)(2, 5)(3, 6)$  swaps the factors  $(1, 2, 3)$  and  $(4, 5, 6)$ .

$$C = \langle (1, 2, 3), (4, 5, 6), (1, 4)(2, 5)(3, 6) \rangle$$

- (iv) Now any permutation of the three 3-cycles is allowed. We may get all permutation of three symbols by composing a transposition and a 3-cycle of the symbols. A transposition is effected by  $(1, 4)(2, 5)(3, 6)$  while a three cycle is effected by  $(1, 4, 7)(2, 5, 8)(3, 6, 9)$ .

$$C = \langle (1, 2, 3), (4, 5, 6), (7, 8, 9), (1, 4)(2, 5)(3, 6), (1, 4, 7)(2, 5, 8)(3, 6, 9) \rangle$$

$$(i) \quad \langle (1, 2), (1, 2, 3) \rangle$$

$$(ii) \quad \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$$

$$(iii) \quad \langle (1, 2, 3), (2, 3, 4) \rangle$$

$$(iv) \quad \langle (1, 2, 3, 4), (1, 4, 2) \rangle$$

*Solution.*

Let  $X$  be a subset of the finite group  $G$ . If  $H$  is a subgroup of  $G$  such that  $H \subseteq \langle X \rangle$  and  $HX \subseteq H$ , then it follows that  $H = \langle X \rangle$ . (Why is this so?) This fact suggests an algorithm for computing  $\langle X \rangle$ : Suppose that  $X = \{x_1, \dots, x_n\}$  and we know  $K = \langle \{x_1, \dots, x_{n-1}\} \rangle$ . If  $KX \subseteq K$ , then  $\langle X \rangle = K$ , otherwise set  $H = K$  and joint to  $H$  (disjoint) cosets of  $K$  until  $HX \subseteq H$  holds.

(i) Let  $H = \langle (1, 2), (1, 2, 3) \rangle$ . Since  $(1, 2)$  and  $(1, 2, 3)$  have orders 2 and 3 respectively, the order of  $H$  must be divisible by 2 and 3. Hence 6 divides  $|H|$ . Conversely,  $H \leq S_3$  and  $S_3$  has order  $3! = 6$ , so  $H = S_3$ . An alternative approach using the above algorithm is to set  $K = \langle (1, 2) \rangle$ . Then the cosets  $K, K(1, 2, 3)$  and  $K(1, 3, 2)$  are disjoint. Set  $H = K \cup K(1, 2, 3) \cup K(1, 3, 2)$ . Then  $H(1, 2) \subseteq H$  and  $H(1, 2, 3) \subseteq H$ . Hence  $H = \langle (1, 2), (1, 2, 3) \rangle$ .

(ii) The above algorithm yields

$$\langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle = \{\iota, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

If  $a = (1, 2)(3, 4)$  and  $b = (1, 3)(2, 4)$  then it is easy to see that  $a^2 = b^2 = \iota$ ,  $ab = ba$  and  $a \neq b$ . Hence,  $\langle a, b \rangle = \{\iota, a, b, ab\}$ .

(iii) Set  $K = \langle (1, 2, 3) \rangle$ . The cosets  $K, K(2, 3, 4)$  and  $K(2, 4, 3)$  are disjoint (why?) so their union contains 9 elements. Therefore  $\langle (1, 2, 3), (2, 3, 4) \rangle$  has order  $\geq 9$ . But this subgroup is contained in  $A_4$  and so has order divisible by 12, hence it equals  $A_4$ .

(iv) The order of this subgroup is divisible by 4 and 3 and hence is a multiple of 12. Now  $S_4$  has only two subgroups whose order is a multiple of 12, namely  $A_4$  and  $S_4$ . Since  $(1, 2, 3, 4)$  is odd,  $\langle (1, 2, 3, 4), (1, 4, 2) \rangle = S_4$ . One can reach the same conclusion using the algorithm above, although more work is required.

**55.** Prove that the elementary matrices generate  $GL_n$ . (Recall from linear algebra that the elementary matrices are the matrices you obtain from the identity matrix by applying elementary row or column operations.)

*Solution.*

It is a well-known fact from linear algebra that a matrix  $A$  can be factored as  $A = E_r \cdots E_2 E_1 B$  where the  $E_i$ ,  $1 \leq i \leq r$ , are elementary matrices and  $B$  is the

**56.** Find the right cosets of  $H$  in  $G$  where

(i)  $G = \mathbb{Z}_{10}$  and  $H = \langle 2 \rangle$ ,                      (ii)  $G = \mathbb{Z}_{12}$  and  $H = \langle 4 \rangle$ ,

(iii)  $G = D_8 = \langle (1, 2)(3, 4), (1, 2, 3, 4) \rangle$  and  $H = \langle (1, 2)(3, 4) \rangle$ .

*Solution.*

(i)  $H = \{0, 2, 4, 6, 8\}$  and  $H + 1 = \{1, 3, 5, 7, 9\}$ .

(ii)  $H = \{0, 4, 8\}$ ,  $H + 1 = \{1, 5, 9\}$ ,  $H + 2 = \{2, 6, 10\}$ ,  $H + 3 = \{3, 7, 11\}$ .

(iii)

$$\begin{aligned} H\iota &= \{\iota, (1, 2)(3, 4)\}, \\ H(1, 2, 3, 4) &= \{(1, 2, 3, 4), (2, 4)\}, \\ H(1, 2, 3, 4)^2 &= H(1, 3)(2, 4) = \{(1, 3)(2, 4), (1, 4)(2, 3)\}, \\ H(1, 2, 3, 4)^3 &= H(1, 4, 3, 2) = \{(1, 4, 3, 2), (1, 3)\}. \end{aligned}$$

**57.** Let  $H \leq G$  and  $x, y \in G$ .

(i) Show that the following are equivalent:

$$Hx = Hy, Hxy^{-1} = H, xy^{-1} \in H.$$

(ii) Show that the following are equivalent:

$$xH = yH, y^{-1}xH = H, y^{-1}x \in H.$$

*Solution.*

(i) Now  $Hx = Hy$  iff  $Hxy^{-1} = Hyy^{-1} = H$ . If  $Hxy^{-1} = H$ , then  $xy^{-1} = e xy^{-1} \in Hxy^{-1} = H$ . Conversely, if  $xy^{-1} \in H$ , then  $h \mapsto hxy^{-1}$  is a permutation of  $H$  (c.f. Cayley's theorem), so  $Hxy^{-1} = H$ .

(ii) Similar to (i).

*Solution.*

The cosets of  $m\mathbb{Z}$  in  $\mathbb{Z}$  are  $x+m\mathbb{Z}$ ,  $0 \leq x < m$ . These can be shown to be distinct. Hence  $|\mathbb{Z} : m\mathbb{Z}| = m$ .

59. Suppose that  $H$  and  $K$  are subgroups of  $G$  and that  $H \subseteq K$ . Choose representatives  $x_1, x_2, \dots, x_m$  for the right cosets of  $H$  in  $K$ , and representatives  $y_1, y_2, \dots, y_n$  for the right coset of  $K$  in  $G$ . Show that the elements  $x_i y_j$ ,  $1 \leq i \leq m$ ,  $1 \leq j \leq n$ , are representatives for the right cosets of  $H$  in  $G$ . Deduce that

$$|G : H| = |G : K| \cdot |K : H|.$$

*Solution.*

The above formula may be deduced easily from Lagrange's theorem. The purpose of this question is to show what happens to the coset representatives. Let the symbol  $\sqcup$  denote disjoint union. If we substitute the equation

$$(1) \quad K = Hx_1 \sqcup \dots \sqcup Hx_m$$

into the equation

$$(2) \quad G = Ky_1 \sqcup \dots \sqcup Ky_n$$

we see that  $G$  is the disjoint union of the  $Hx_i y_j$ ,  $1 \leq i \leq m$ ,  $1 \leq j \leq n$ . A more formal proof proceeds as follows. Let  $g \in G$ . Then  $g \in Ky_j$  for some  $j$  by (2). Hence  $y_j^{-1}g \in K$  and so  $y_j^{-1}g \in Hx_i$  for some  $i$  by (1). Thus  $g \in Hx_i y_j$ . Suppose that  $g \in Hx_i y_j \cap Hx_k y_l$ . Then  $g \in Ky_j \cap Ky_l$  so  $j = l$  by (2). Hence  $gy_j^{-1} \in Hx_i \cap Hx_k$  and by (1),  $i = k$ . We have now shown that the  $Hx_i y_j$  form a partition of  $G$  as desired.

60. Let  $G$  be a nontrivial group whose only subgroups are  $\{1\}$  and  $G$ . Show that  $G$  is cyclic of prime order.

*Solution.*

This is the converse of the theorem: The only subgroups of a group  $G$  of prime order are  $\{e\}$  and  $G$ . Since  $G$  is nontrivial, there is a nontrivial element  $x$  in  $G$ . Since  $\langle x \rangle \neq \{e\}$ , it follows that  $\langle x \rangle = G$ . Hence  $G$  is cyclic. If  $G = \langle x \rangle$  has infinite order, then  $\langle x^2 \rangle$  is a proper nontrivial subgroup. This can not happen, so  $G$  has finite order  $n$ . If  $n$  is composite, then  $n = ab$  where  $1 < a, b < n$ . Thus  $\langle x^a \rangle$  is a proper subgroup of order  $b$ . This can not occur so  $G$  must be cyclic of prime order.

of rotations and reflections that preserve a regular  $n$ -gon is such a group and has order exactly  $2n$ .

*Solution.*

If we show that  $G$  equals

$$(1) \quad \{e, b, \dots, b^{n-1}, a, ab, \dots, ab^{n-1}\},$$

then it follows that  $|G| \leq 2n$  as the above elements need not be distinct. We must show that the rules  $a^2 = b^n = 1$  and  $ba = ab^{-1}$  are sufficient for writing every word in the elements  $a, a^{-1}, b, b^{-1}$ , in the form  $a^i b^j$  where  $0 \leq i < 2$  and  $0 \leq j < n$ . Since  $a^{-1} = a$  and  $b^{-1} = b^{n-1}$  we need only consider words in  $a$  and  $b$ . It follows from  $ba = ab^{n-1}$  that  $b^y a = ab^{(n-1)y}$ . Hence we can push the  $a$ 's past the  $b$ 's and so every word in  $a$  and  $b$  can be written in the form  $a^i b^j$ . The rules  $a^2 = b^n = 1$  allow us to assume  $0 \leq i < 2$  and  $0 \leq j < n$ .

Consider a regular  $n$ -gon with vertices  $1, 2, \dots, n$ . Then the permutations

$$a = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix} = (1, n)(2, n-1) \cdots \quad \text{and}$$

$$b = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix} = (1, 2, \dots, n)$$

satisfy the rules  $a^2 = b^n = 1$  and  $ba = ab^{-1}$ , and since  $a \notin \langle b \rangle$ , the cosets  $\langle b \rangle$  and  $a\langle b \rangle$  are disjoint and both have  $n$  elements. Hence  $|\langle a, b \rangle| \geq 2n$ . Combined with the previous paragraph, we see  $|\langle a, b \rangle| = 2n$ . Some authors denote the dihedral group of order  $2n$  by  $D_{2n}$  while others denote it by  $D_n$ , so be careful!

**62.** If a group  $Q$  is generated by two elements  $a$  and  $b$  satisfying

$$a^4 = 1, \quad a^2 = b^2, \quad \text{and} \quad ba = ab^3,$$

show that  $|Q| \leq 8$ . Verify that the subgroup of  $\text{GL}(2, \mathbf{C})$  generated by the matrices

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

has order 8 and satisfies the rules above. We called  $Q$  the *quaternion group* of order 8.

*Solution.*

An argument similar to that in exercise 61 shows that  $Q$  has at most 8 distinct elements namely

$$\{1, b, b^2, b^3, a, ab, ab^2, ab^3\}.$$

It is straightforward to verify that  $A^2 = B^2 = -I$  and  $BA = AB^3$ . Since  $A \notin \langle B \rangle$ , it follows that  $\langle A, B \rangle$  has order  $\geq 8$ . Since  $|Q| \leq 8$ , it follows that  $\langle A, B \rangle$  has order precisely 8.

forms a group under the binary operation

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2).$$

This is called the *direct product* of  $G$  and  $H$ .

*Solution.*

Closure holds since  $g_1g_2 \in G$  and  $h_1h_2 \in H$ . The associative law follows from the associative laws in  $G$  and in  $H$ . The identity element is  $(e_G, e_H)$  where  $e_G$  and  $e_H$  are the identity elements of  $G$  and  $H$  respectively. The inverse of  $(g, h)$  is  $(g^{-1}, h^{-1})$ . Hence  $G \times H$  is a group. A simple counting argument shows  $|G \times H| = |G| \cdot |H|$ .

**64.** Which of the following are functions, and of those, which are homomorphisms. For each homomorphism determine its kernel and image.

(i)  $\phi: \mathbb{Z}_3^+ \times \mathbb{Z}_4^+ \rightarrow \mathbb{Z}_{12}^+ : (x + 3\mathbb{Z}, y + 4\mathbb{Z}) \mapsto x + y + 12\mathbb{Z},$

(ii)  $\phi: \mathbb{Z}_{12}^+ \rightarrow \mathbb{Z}_3^+ \times \mathbb{Z}_4^+ : x + 12\mathbb{Z} \mapsto (x + 3\mathbb{Z}, x + 4\mathbb{Z}),$

(iii)  $\phi: \mathbb{Z}_{12}^\times \rightarrow \mathbb{Z}_3^\times \times \mathbb{Z}_4^\times : x + 12\mathbb{Z} \mapsto (x + 3\mathbb{Z}, x + 4\mathbb{Z}),$

(iv)  $\phi: \mathbb{C}^\times \rightarrow \mathbb{C}^\times : x \mapsto x^3$ , where  $\mathbb{C}^\times$  is the group of nonzero complex numbers under multiplication,

(v)  $\phi: \mathbb{R}^\times \rightarrow \mathbb{R}^\times : x \mapsto 2^x,$

(vi)  $\phi: \mathbb{Q}^+ \rightarrow \mathbb{C}^\times : x \mapsto e^{2\pi ix},$

(vii)  $\phi: \mathbb{Z}_{12}^+ \rightarrow \mathbb{Z}_{12}^+ : x \mapsto 3x.$

*Solution.*

(i) This is not a well-defined function! Note that  $(0 + 3\mathbb{Z}, 0 + 4\mathbb{Z}) = (3 + 3\mathbb{Z}, 0 + 4\mathbb{Z})$  but  $\phi(0 + 3\mathbb{Z}, 0 + 4\mathbb{Z}) \neq \phi(3 + 3\mathbb{Z}, 0 + 4\mathbb{Z})$ .

(ii) This function is well-defined: if  $x + 12\mathbb{Z} = x' + 12\mathbb{Z}$ , then it follows that  $x + 3\mathbb{Z} = x' + 3\mathbb{Z}$  and  $x + 4\mathbb{Z} = x' + 4\mathbb{Z}$ . Furthermore,  $\phi$  is a homomorphism as

$$\phi(x + y) = (x + y, x + y) = (x, x) + (x, y) = \phi(x) + \phi(y).$$

$\ker(\phi) = \{0\}$  (i.e.  $\phi$  is injective) and  $\text{im}(\phi) = \mathbb{Z}_3 \times \mathbb{Z}_4$  (i.e.  $\phi$  is surjective).

$$\phi(xy) = (xy, xy) = (x, x)(x, y) = \phi(x)\phi(y).$$

Also  $\phi$  is an isomorphism.

(iv) Since  $(xy)^3 = x^3y^3$ ,  $\phi$  is a homomorphism. Also

$$\ker(\phi) = \{1, e^{2\pi i/3}, e^{4\pi i/3}\} \quad \text{and} \quad \text{im}(\phi) = \{\mathbf{C}^\times\}.$$

Recall that  $|\ker(\phi)|$  determines the number of times  $G$  is “wrapped” around the image  $\text{im}(\phi)$ . In this example, the infinite set  $\mathbf{C}^\times$  is wrapped around itself three times. Note that we can only have  $3|G| = |G|$  if  $|G| = \infty$  as we do in this example.

(v)  $\phi$  is not a homomorphism since  $\phi(1) = 2$ . That is,  $\phi$  does not map the identity element of the domain to the identity element of the codomain. Note that

$$\phi: \mathbb{R}^+ \rightarrow \mathbb{R}^\times : x \mapsto 2^x$$

is a homomorphism.

(vi) Since  $e^{2\pi i(x+y)} = e^{2\pi ix}e^{2\pi iy}$ ,  $\phi$  is a homomorphism. Furthermore,

$$\ker(\phi) = \mathbf{Z} \quad \text{and} \quad \text{im}(\phi) = \{e^{2\pi ix} \mid x \in \mathbf{Q}\}.$$

Can you show that although  $\text{im}(\phi)$  is a *proper* subgroup of the unit circle  $\{z \mid |z| = 1\}$ , it is not equal?

(vii)  $\phi$  is a homomorphism since

$$\phi(x + y) = 3(x + y) = 3x + 3y = \phi(x) + \phi(y).$$

$$\ker(\phi) = \langle 4 \rangle \quad \text{and} \quad \text{im}(\phi) = \langle 3 \rangle.$$

**65.** Show that a group  $G$  is abelian if and only if the map  $\phi: G \rightarrow G: x \mapsto x^2$  is a homomorphism.

*Solution.*

If  $G$  is abelian, then  $xy = yx$  for all  $x, y \in G$ . It follows that  $(xy)^n = x^n y^n$  for all  $n \in \mathbf{Z}$ . Putting  $n = 2$  shows that  $\phi$  is a homomorphism. Conversely, suppose that  $\phi$  is a homomorphism. Then for all  $x, y \in G$ , we have  $(xy)^2 = x^2 y^2$ . By exercise 15,  $G$  is abelian.

example in which  $H$  is normal in  $G$  but  $\phi(H)$  is not normal in  $G'$ .

- (ii) If  $H'$  is a subgroup of  $G'$ , show that the preimage

$$H = \phi^{-1}(H') = \{h \in G \mid \phi(h) \in H'\}$$

is a subgroup of  $G$ . If  $H'$  is a normal subgroup of  $G'$ , is it true that  $H$  is a normal subgroup of  $G$ ?

*Solution.*

- (i)  $e' = \phi(e) \in \phi(H)$  so  $\phi(H)$  is nonempty. Suppose  $\phi(h_1)$  and  $\phi(h_2)$  are elements of  $H'$ , where  $h_1, h_2 \in H$ . Then

$$\phi(h_1)\phi(h_2)^{-1} = \phi(h_1)\phi(h_2^{-1}) = \phi(h_1h_2^{-1}) \in \phi(H)$$

as  $h_1h_2^{-1} \in H$ . Hence  $\phi(H)$  is a subgroup of  $G'$ . There is a homomorphism  $\phi: S_3 \rightarrow S_3$  whose kernel is  $A_3$  and whose image is  $\langle (1, 2) \rangle$ . Clearly  $S_3 \trianglelefteq S_3$  but  $\phi(S_3)$  is not normal in  $S_3$ . (If  $\phi$  is surjective, then this can never happen.)

- (ii) Now  $H$  is nonempty as  $e \in H$  because  $\phi(e) = e' \in H'$ . If  $h_1, h_2 \in H$ , then  $\phi(h_1), \phi(h_2) \in H'$ . Since  $H' \leq G'$ , we have  $\phi(h_1h_2^{-1}) = \phi(h_1)\phi(h_2)^{-1} \in H'$ . Hence  $H \leq G$ . If  $H' \trianglelefteq \text{im}(\phi)$ , then it follows that  $H \trianglelefteq G$ . The converse is also true.

**67.** Define  $\phi: \mathbb{Z}_6 \rightarrow S_3$  by  $i \mapsto (1, 2, 3)^i$ .

- (i) Show that  $\phi$  is a homomorphism.  
(ii) Determine the kernel and image of  $\phi$ .

*Solution.*

First,  $\phi$  is well-defined since  $i + 6\mathbb{Z} = j + 6\mathbb{Z}$  implies that  $(1, 2, 3)^i = (1, 2, 3)^j$ . Indeed, if  $i + 3\mathbb{Z} = j + 3\mathbb{Z}$  then we could reach the same conclusion.  $\phi$  is a homomorphism since

$$\phi(i + j) = (1, 2, 3)^{i+j} = (1, 2, 3)^i(1, 2, 3)^j = \phi(i)\phi(j).$$

$\ker(\phi) = \langle 3 \rangle$  and  $\text{im}(\phi) = \langle (1, 2, 3) \rangle$ .

*Solution.*

No! All we can say is  $ghg^{-1} \in H$ . If  $G = S_3$ ,  $H = A_3$ ,  $g = (2, 3)$  and  $h = (1, 2, 3)$ , then

$$ghg^{-1} = (2, 3)(1, 2, 3)(2, 3)^{-1} = (1, 3, 2) \neq (1, 2, 3).$$

(If  $H$  is a normal subgroup of order 2, or more generally if  $H$  is a subgroup of the centre of  $G$ , then we can make this conclusion (why?).)

**69.** Let  $\mathbf{C}^\times$  and  $\mathbb{R}^{>0}$  denote the set of nonzero complex numbers and the positive real numbers with the binary operation of multiplication. Show that

$$\phi: \mathbf{C}^\times \rightarrow \mathbb{R}^{>0}: z \mapsto |z|$$

is a homomorphism. Find  $\ker(\phi)$  and describe the cosets of  $\ker(\phi)$  in geometric terms.

*Solution.*

Let  $z_1 = x_1 + y_1i$  and  $z_2 = x_2 + y_2i$ , where  $x_1, x_2, y_1, y_2 \in \mathbb{R}$ . Then

$$\begin{aligned} |z_1 z_2| &= |(x_1 + y_1i)(x_2 + y_2i)| \\ &= |(x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)i| \\ &= \sqrt{(x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2} \\ &= \sqrt{(x_1^2 + x_2^2)(y_1^2 + y_2^2)} \\ &= \sqrt{x_1^2 + x_2^2} \sqrt{y_1^2 + y_2^2} \\ &= |z_1| |z_2|. \end{aligned}$$

Hence  $\phi$  is a homomorphism. (Note that a complex number  $z$  is commonly represented in rectangular form  $x + yi$ , or in polar form  $re^{i\theta}$ , where  $r = \sqrt{x^2 + y^2}$  and  $\theta$  is the angle from the positive  $x$ -axis to  $z$  i.e.  $\tan^{-1}(y/x)$  or  $\pi + \tan^{-1}(y/x)$ . The rectangular form is most convenient for adding, while the polar form is best for multiplying as  $r_1e^{i\theta_1}r_2e^{i\theta_2} = r_1r_2e^{i(\theta_1+\theta_2)}$ .) Note that  $\text{im}(\phi) = \mathbb{R}^{>0}$  and  $\ker(\phi)$  is the unit circle  $S^1 = \{z \mid |z| = 1\}$ . If  $r \in \mathbb{R}^{>0}$ , then the circle  $\{z \mid |z| = r\}$ , centered at 0 of radius  $r$ , is the coset  $r\ker(\phi)$ . (Can you interpret the group isomorphism  $\mathbf{C}^\times \cong \mathbb{R}^{>0} \times S^1$  geometrically?)

**70.** Prove that  $\phi: \mathbb{R}^+ \rightarrow \mathbb{R}^{>0}: x \mapsto e^x$  is an isomorphism and describe  $\phi^{-1}$ .

*Solution.*

Since  $e^{x_1+x_2} = e^{x_1}e^{x_2}$ ,  $\phi$  is a homomorphism. The map  $\mathbb{R}^{>0} \rightarrow \mathbb{R}^+: y \mapsto \log(y)$  is the inverse of the function  $\phi$ , hence  $\phi$  is an isomorphism.

*Solution.*

The way to show that two groups  $G$  and  $H$  are not isomorphic, is to find an *invariant* of  $G$  which is different to an invariant of  $H$ . By an invariant, we mean a group theoretic property that is shared by isomorphic groups. For example, being abelian, being cyclic, having the same order, having the same number of elements of a given order, etc. Now  $\mathbb{R}^+$  has no elements of order 2, but  $\mathbb{R}^{>0}$  has one element, namely  $-1$ . Hence  $\mathbb{R}^+ \not\cong \mathbb{R}^{>0}$ .

**72.** Prove that  $\mathbb{R}^\times$  is isomorphic to  $\{-1, 1\} \times \mathbb{R}^{>0}$ .

*Solution.*

If  $x \in \mathbb{R}^\times$  there is a unique number called  $\text{sign}(x)$  satisfying  $x = \text{sign}(x)|x|$ . Clearly  $\text{sign}(x) = \pm 1$ . Furthermore, if  $x_1, x_2 \in \mathbb{R}$ , then

$$\text{sign}(x_1x_2)|x_1x_2| = x_1x_2 = \text{sign}(x_1)|x_1|\text{sign}(x_2)|x_2|,$$

and it follows that  $\text{sign}(x_1x_2) = \text{sign}(x_1)\text{sign}(x_2)$  and  $|x_1x_2| = |x_1| \cdot |x_2|$ . Hence one can show that

$$\phi: \mathbb{R}^\times \rightarrow \{-1, 1\} \times \mathbb{R}^{>0}: x \mapsto (\text{sign}(x), |x|)$$

is an isomorphism. Note that  $\phi$  is obtained by “gluing” together the homomorphisms  $x \mapsto \text{sign}(x)$  and  $x \mapsto |x|$  of  $\mathbb{R}^\times$ .

**73.** Prove that  $\mathbb{Z}_2 \times \mathbb{Z}_3$  is cyclic and hence is isomorphic to  $\mathbb{Z}_6$ .

*Solution.*

The order of  $(1 + 2\mathbb{Z}, 1 + 3\mathbb{Z}) \in \mathbb{Z}_2 \times \mathbb{Z}_3$  is 6. Hence

$$\phi: \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3: x + 6\mathbb{Z} \mapsto (x + 2\mathbb{Z}, x + 3\mathbb{Z})$$

is an isomorphism. (Is it clear why  $\phi$  is well-defined, a homomorphism, injective and surjective?) Note that  $\phi^{-1}(1, 0) = 3$  and  $\phi^{-1}(0, 1) = 4$  hence the inverse isomorphism is

$$\phi^{-1}: \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_6: (x, y) \mapsto 3x + 4y.$$

Note that  $(1 + 2\mathbb{Z}, 2 + 3\mathbb{Z})$  is the other generator for  $\mathbb{Z}_2 \times \mathbb{Z}_3$ .

your isomorphism is well-defined.)

\*(iii) If  $\gcd(m, n) = 1$ , then describe the inverse isomorphism

$$\phi^{-1}: \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{mn}.$$

*Solution.*

(i) Compare with exercise 73. The order of the element  $(1 + m\mathbb{Z}, 1 + n\mathbb{Z})$  is a multiple of  $m$  and of  $n$ . Since  $\gcd(m, n) = 1$ , it follows that its order is  $mn$ . Therefore

$$\phi: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n: x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

is a well-defined isomorphism.

(ii) Now  $\phi(10) = (1, 0)$  and  $\phi(6) = (0, 1)$ . Hence

$$\phi^{-1}(x, y) = x\phi^{-1}(1, 0) + y\phi^{-1}(0, 1) = 10x + 6y.$$

(iii) Motivated by the previous part, we seek integers  $M$  and  $N$  such that  $\phi(M) = (1, 0)$  and  $\phi(N) = (0, 1)$ , then  $\phi^{-1}(x, y) = xM + yN$ . Euclid's algorithm, for finding greatest common divisors, may be used to find integers  $a$  and  $b$  such that  $am + bn = 1$ . Then we can take  $M = bn$  and  $N = am$  (why?). Hence  $\phi^{-1}(x, y) = bnx + amy$ . This isomorphism is frequently called the Chinese remainder theorem. Note that  $\phi$  and  $\phi^{-1}$  induce isomorphisms  $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$  and  $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times \cong \mathbb{Z}_{mn}^\times$ . These results are false if you drop the assumption that  $\gcd(m, n) = 1$ .

**75.** Show that  $\mathbb{Z} \times \mathbb{Z}$  and  $\mathbb{Z}$  are not isomorphic.

*Solution.*

Suppose that  $\phi: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$  is an isomorphism. Since  $\phi$  preserves addition,  $\phi(n) = n\phi(1)$  for all  $n \in \mathbb{Z}$ . If  $\phi(1) = (x, y)$ , then  $\text{im}(\phi) = \{(nx, ny) \mid n \in \mathbb{Z}\}$ . Since  $\phi$  is surjective,  $(1, 0) \in \text{im}(\phi)$  and so  $y = 0$ , and  $(0, 1) \in \text{im}(\phi)$  and so  $x = 0$ . Hence  $\phi(1) = (0, 0)$  and  $\phi$  is not injective. This contradiction shows that  $\mathbb{Z} \not\cong \mathbb{Z} \times \mathbb{Z}$ . (Note the elements of the set  $\{n\phi(1) \mid n \in \mathbb{Z}\}$  lie on a dotted straight line which can clearly never equal the dotted plane  $\mathbb{Z} \times \mathbb{Z}$ . In general,  $\mathbb{Z}^m$ , the direct product of  $m$  copies of  $\mathbb{Z}$ , is not isomorphic to  $\mathbb{Z}^n$  if  $m \neq n$ . Note that  $2\mathbb{Z}^m$  has  $2^m$  cosets in  $\mathbb{Z}^m$  and similarly,  $2\mathbb{Z}^n$  has  $2^n$  cosets in  $\mathbb{Z}^n$ . Any isomorphism  $\mathbb{Z}^m \rightarrow \mathbb{Z}^n$  would map  $2\mathbb{Z}^m$  to  $2\mathbb{Z}^n$ , so there can be no such isomorphism unless  $m = n$ . Note that  $\mathbb{Z}/2\mathbb{Z}^n$  is an  $n$ -dimensional vector space over the field  $\mathbb{Z}_2$ .)

*Solution.*

The map  $\phi: G \rightarrow G \times G: x \mapsto (x, x)$  is easily seen to be an injective homomorphism whose image is  $D$ . Hence  $D$  is a subgroup of  $G \times G$  and  $G \cong D$ .

**77.** Let  $D_{2n}$  denote the dihedral group of order  $2n$ , which by exercise 61 is the group of symmetries of a regular  $n$ -gon.

(i) Show that a symmetry of a regular hexagon either fixes or inverts an inscribed equilateral triangle.

\*(ii) Describe homomorphisms  $\phi_1: D_{12} \rightarrow \mathbf{Z}_2$  and  $\phi_2: D_{12} \rightarrow D_6$  and hence find an isomorphism  $\phi: D_{12} \rightarrow \mathbf{Z}_2 \times D_6$ .

*Solution.*

(i) Let the vertices of a regular hexagon be numbered  $1, 2, \dots, 6$  in some direction. The vertices  $1, 3, 5$  and the vertices  $2, 4, 6$  describe equilateral triangles. A symmetry of the hexagon either fixes both of these triangles or its negative does. Essentially we have a geometric realization here of a homomorphism  $D_{12} \rightarrow D_6$ .

(ii) Recall that the elements of  $D_{2n}$  have the form  $a^i b^j$  where  $0 \leq i < 2$  and  $0 \leq j < n$ . Multiplication is carried out using the rules  $a^2 = b^n = 1, ba = ab^{-1}$ . Indeed, one may deduce an explicit rule for multiplication namely  $(a^i b^j)(a^{i'} b^{j'}) = a^{i''} b^{j''}$ , where  $i'' = i + i' \pmod{2}$  and  $j'' = (-1)^{i'} j + j' \pmod{n}$ . Suppose now that  $n = 6$ . Suppose that  $a$  is a reflection which maps the equilateral triangle to itself. Then  $a^i b^j$  maps the triangle to itself if and only if  $j$  is even. Therefore

$$\phi_1: a^i b^j \mapsto j + 2\mathbf{Z}$$

is a homomorphism. Similarly,  $b^2$  also maps the triangle to itself, and

$$\phi_2: a^i b^j \mapsto a^i b^{2j}$$

is a homomorphism. Then  $\phi(a^i b^j) = (\phi_1(a^i b^j), \phi_2(a^i b^j))$  defines a homomorphism. It is not hard to verify that  $\phi$  is injective and thus an isomorphism. (In general,  $D_{4n} \cong \mathbf{Z}_2 \times D_{2n}$  if  $n$  is odd.)

*Solution.*

By definition  $\phi$  is a bijection and hence there is an inverse function  $\phi^{-1}$  which is also a bijection. The purpose of this exercise is to verify that  $\phi^{-1}$  preserves products and so is a homomorphism. Suppose that  $\phi(x_1) = y_1$  and  $\phi(x_2) = y_2$ . We want to show that  $\phi^{-1}(y_1y_2) = \phi^{-1}(y_1)\phi^{-1}(y_2)$ . Since  $\phi$  is a homomorphism,  $\phi(x_1x_2) = \phi(x_1)\phi(x_2) = y_1y_2$ . Hence  $x_1x_2 = \phi^{-1}(y_1y_2)$  or  $\phi^{-1}(y_1y_2) = \phi^{-1}(y_1)\phi^{-1}(y_2)$ .

**79.** If  $\phi: G \rightarrow G'$  is an isomorphism and  $x \in G$ , show that  $\phi(x)$  and  $x$  have the same order.

*Solution.*

If the powers of  $x$  are all distinct, then as  $\phi$  is injective, so are the powers of  $\phi(x)$ . Hence if  $|x| = \infty$ , then  $|\phi(x)| = \infty$ . Suppose now that  $|x| = n$  is finite. It suffices to show that  $|x|$  divides  $|\phi(x)|$  and  $|\phi(x)|$  divides  $|x|$ . The second statement follows because

$$\phi(x)^n = \phi(x^n) = \phi(e) = e'.$$

And the first statement follows using a similar argument and the fact that  $\phi^{-1}$  is an isomorphism.

**80.** If  $\phi: G \rightarrow G$  is a homomorphism, show that  $\{x \in G \mid \phi(x) = x\}$  is a subgroup of  $G$ . What is this subgroup when  $\phi: \text{GL}(n, \mathbb{R}) \rightarrow \text{GL}(n, \mathbb{R}) : A \mapsto (A^{-1})^t$ ?

*Solution.*

Let  $H = \{x \in G \mid \phi(x) = x\}$ . Clearly  $e \in H$ . If  $x, y \in H$ , then  $\phi(x) = x$  and  $\phi(y) = y$ . Hence

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = xy^{-1}$$

so  $xy^{-1} \in H$  and it follows that  $H \leq G$ .

If  $\phi$  is the above map, then it follows from well-known properties of transpose and trace (namely  $(AB)^t = B^tA^t$  and  $(AB)^{-1} = B^{-1}A^{-1}$ ) that  $\phi$  is a homomorphism. (Indeed,  $\phi$  is an isomorphism called the *contragredient* isomorphism.) Now  $A \in H$  iff  $(A^{-1})^t = A$ . That is iff  $A$  is an orthogonal matrix. (Hence the set of orthogonal matrices forms a group.)

*Solution.*

Recall that two permutations in  $S_n$  are conjugate if and only if they have the same disjoint cycle structure. I will list the size of the conjugacy classes and a typical element of it.

$$\left( \begin{array}{cccccc} \iota & (a, b) & (a, b, c) & (a, b, c, d) & (a, b)(c, d) \\ 1 & \frac{4 \cdot 3}{2} = 6 & \frac{4 \cdot 3 \cdot 2}{3} = 8 & \frac{4!}{4} = 6 & \frac{1}{2!} \frac{4 \cdot 3}{2} \frac{2 \cdot 1}{2} = 3 \end{array} \right).$$

Note that the total number of elements is  $24 = 4!$ . This is a good check. The normal subgroups are unions of conjugacy classes. By Lagrange's theorem, the order of a subgroup divides 24. The possible orders of normal subgroups in this example are 1, 4, 12 and 24. (These are the only numbers which divide 24 and are a sum of 1 and some of the numbers 6, 8, 6, 3.) The only normal subgroup candidates are: class 1, the union of class 1 and class 5, the union of classes 1, 3, 5, and the union of all the classes. Each of these candidates yields a normal subgroup. They are  $\{\iota\}$ ,  $V$ ,  $A_4$ ,  $S_4$  respectively.

- \*82. Find all of the conjugacy classes, all of the normal subgroups and all of the homomorphic images of  $S_5$ .

*Solution.*

This question is similar to exercise 81. The classes and their sizes are:

$$\left( \begin{array}{cccccccc} \iota & (a, b) & (a, b, c) & (a, b, c, d) & (a, b, c, d, e) & (a, b)(c, d) & (a, b, c)(d, e) \\ 1 & 10 & 20 & 30 & 24 & 15 & 20 \end{array} \right).$$

As a check, note that there are  $60 = 5!/2$  even permutations and 60 odd permutations. Since the transpositions generate  $S_5$ , a normal subgroup containing the second class must be  $S_5$ . Since the 3-cycles generate  $A_5$ , a normal subgroup containing the third class contains  $A_5$ . A normal subgroup containing the fourth class contains  $(1, 4, 3, 2)(1, 3, 2, 4) = (1, 2, 3)$  and hence contains  $A_5$ . Such a subgroup contains  $A_5$  and the odd permutation  $(1, 2, 3, 4)$  and so must be  $S_5$ . Similarly, a normal subgroup containing the fifth class contains  $(1, 2, 3, 4, 5)(1, 2, 5, 4, 3) = (1, 3, 2)$  and hence contains  $A_5$ . A normal subgroup containing the class  $(a, b)(c, d)$  must also contain  $(1, 2)(4, 5)(1, 3)(4, 5) = (1, 2, 3)$ , and hence must contain  $A_5$ . Similarly, a normal subgroup containing the class  $(a, b, c)(d, e)$  must contain

$$(1, 2, 3)(4, 5)(1, 2, 3)(4, 5) = (1, 3, 2)$$

and hence contain  $A_5$ . Since  $(a, b, c)(d, e)$  is odd, this normal subgroup has  $> 60$  elements and so equals  $S_5$ . In summary, any normal subgroup containing a nontrivial conjugacy class contains either  $A_5$  or  $S_5$ . Hence the normal subgroups of  $S_5$  are  $1, A_5, S_5$ . (If  $n \geq 5$ , the normal subgroups of  $S_n$  are  $1, A_n, S_n$ . Also, and this does not follow from the previous sentence, the normal subgroups of  $A_n$ ,  $n \geq 5$ , are  $1$  and  $A_n$ .)

(ii) if  $G$  is cyclic, then  $G/N$  is cyclic.

*Solution.*

(i) If  $xy = yx$  for all  $x, y \in G$ , then it follows that

$$xNyN = xyN = yxN = yNxn.$$

Hence  $G/N$  is also abelian.

(ii) If  $G = \langle x \rangle$ , then  $G/N = \langle xN \rangle$  as  $x^iN = (xN)^i$ .

**84.** Find the conjugacy classes of  $D_{10}$ .

*Solution.*

$$\{1\}, \{b, b^{-1}\}, \{b^2, b^{-2}\}, \{a, ab, ab^2, ab^3, ab^4\}.$$

**85.** The *centre* of the group  $G$  is defined to be

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

Find the centre of

(i)  $D_8$

(ii)  $\text{GL}(2, \mathbb{R})$

*Solution.*

(i)  $\{b^2\}$

(ii)  $\{\lambda I \mid \lambda \in \mathbb{R}^\times\}$

**86.** (i) If  $H$  is a subgroup of  $G$  and  $x \in H$ , what can be said about the  $H$ -conjugacy class  $\{h x h^{-1} \mid h \in H\}$  and the  $G$ -conjugacy class  $\{g x g^{-1} \mid g \in G\}$ ?

(ii) If  $H = A_5$  and  $x = (1, 2, 3, 4, 5)$ , find another 5-cycle not  $H$ -conjugate to  $x$ .

*Solution.*

(i) The  $H$ -conjugacy class is contained in the  $G$ -conjugacy class. In some cases we can additionally say that the number of elements of the  $H$ -conjugacy class is divisor of the number of elements of the  $G$ -conjugacy class.

These elements may be found using the substitution rule. Alternatively, they are elements of the left coset

$$(4, 5)C_{S_5}((1, 2, 3, 4, 5)) = (4, 5)\langle(1, 2, 3, 4, 5)\rangle.$$

Each of these is odd so  $x$  and  $y$  are not conjugate in  $A_5$ . In this case the  $A_5$ -conjugacy class containing  $x$  is exactly half the size of the  $S_5$ -conjugacy class containing  $x$ . Can you see any general principles operating here?

**\*87.** Show that the 3-cycles form a single  $A_5$ -conjugacy class.

*Solution.*

The aim of this exercise is to show that two 3-cycles are conjugate by an element of  $A_5$ . (We know they are conjugate by an element of  $S_5$  by the substitution rule.) We shall show that two typical 3-cycles  $(a, b, c)$  and  $(a', b', c')$  are conjugate in  $A_5$ . There are three possibilities. The intersection  $I = \{a, b, c\} \cap \{a', b', c'\}$  has 1, 2 or 3 elements. (Since we are considering permutations of 5 symbols, the intersection can not be empty.) Case (1)  $I = \{a\}$ . In this case  $\{b, c\}$  and  $\{b', c'\}$  are disjoint and the even permutation  $(b, b')(c, c')$  conjugates  $(a, b, c)$  to  $(a, b', c')$ . Case (2)  $I = \{a, b\}$ . Then  $(a', b', c')$  equal  $(a, b, c')$  or  $(a, c', b)$ . Let  $d$  be the symbol which is not  $a, b, c$  or  $c'$ . Then  $(c, c', d)$  conjugates  $(a, b, c)$  to  $(a, b, c')$ . Similarly,  $(b, c', c)$  conjugates  $(a, b, c)$  to  $(a, c', b)$ . In both cases an even permutation will do the required conjugating. Case (3)  $I = \{a, b, c\}$ . In this case  $(a', b', c')$  equals  $(a, b, c)$  or  $(a, c, b)$ . The required even conjugating permutations are  $\iota$  or  $(b, c)(d, e)$  where  $d, e$  are the two symbols not in the set  $\{a, b, c\}$ .

**88.** Find all the normal subgroups of  $D_8$  and hence all of the quotient groups of  $D_8$ .

*Solution.*

This follows from the correspondence theorem and the fact that every nontrivial normal subgroup of  $D_8$  contains the normal subgroup  $\langle b^2 \rangle$  of order 2. There is one normal subgroup of order 8 namely  $D_8 = \langle a, b \rangle$ . There are three of order 4 namely  $\langle a, b^2 \rangle, \langle b \rangle$  and  $\langle ab, b^2 \rangle$ . There is one of order 2:  $\langle b^2 \rangle$ , and one of order 1:  $\{1\}$ . The respective quotient groups are  $\{1\}, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2$ , and  $D_8$ .

*Solution.*

One approach is to note that

$$V = \{\iota\} \cup \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

is a union of conjugacy classes and hence normal. Another approach is to show that  $gVg^{-1} = V$  for all  $g \in S_4$ , or equivalently to show that  $xVx^{-1} = V$  for all  $x$  is a set  $X$  of generators for  $S_4$ . Let  $X$  be the set  $\{(1, 2), (2, 3), (3, 4)\}$  of generators (why?). Then

$$(1, 2)V(1, 2)^{-1} = \langle (2, 1)(3, 4), (2, 3)(1, 4) \rangle = V,$$

$$(2, 3)V(2, 3)^{-1} = \langle (1, 3)(2, 4), (1, 2)(3, 4) \rangle = V,$$

$$(3, 4)V(3, 4)^{-1} = \langle (1, 2)(4, 3), (1, 4)(2, 3) \rangle = V.$$

Hence  $V \trianglelefteq S_4$ .

**90.** If  $H$  is a subgroup of index 2, show that  $H$  is a normal subgroup of  $G$ .

*Solution.*

If  $g \in H$ , then  $gHg^{-1} = H$  holds. If  $g \notin H$ , then  $Hg \neq H$  and  $gH \neq H$ . Thus we can write  $G$  as a disjoint union of cosets of  $H$  in two ways namely  $H \sqcup gH$  and  $H \sqcup Hg$ . It follows that  $gH = Hg$ . Therefore

$$(gH)g^{-1} = (Hg)g^{-1} = H,$$

and so  $H$  is normal in  $G$ . (Hence, for example,  $A_n$  is normal in  $S_n$ , and  $\langle b \rangle$  is normal in  $D_{2n}$ .)

**91.** Let  $H = \{\iota, (1, 2)\}$  and  $K = \{\iota, (1, 3)\}$  be subgroups of  $S_3$ . List the elements of  $HK$  and  $KH$ . Is  $HK$  a subgroup?

*Solution.*

$HK = \{\iota, (1, 2), (1, 3), (1, 3, 2)\}$  and  $KH = \{\iota, (1, 2), (1, 3), (1, 2, 3)\}$ .  $HK$  is not closed under multiplication as  $(1, 3)(1, 2) \notin HK$ , so it is not a group.

*Solution.*

Clearly,  $HK$  is nonempty as  $e = ee \in HK$ . Let  $h_1k_1, h_2k_2 \in HK$  where  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$ . Consider the product  $h_1k_1h_2k_2$ . Since  $KH = HK$ , there exist elements  $h'_2 \in H$  and  $k'_1 \in K$  such that  $k_1h_2 = h'_2k'_1$ . Therefore,

$$h_1k_1h_2k_2 = h_1h'_2k'_1k_2 \in HK.$$

Similarly, if  $hk \in HK$ , then  $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ . So  $HK$  is a nonempty set closed under products and inverses, and hence is a subgroup.

If  $N \trianglelefteq G$ , then  $hNh^{-1} = N$  for all  $h \in H$  so  $hN = Nh$  for all  $h \in H$ . Hence  $HN = NH$  and by the previous part,  $HN$  is a subgroup of  $G$ .

- 93.** If  $M$  and  $N$  are normal subgroups of  $G$ , show that  $M \cap N$  and  $MN$  are normal in  $G$ .

*Solution.*

The intersection of two subgroups is a subgroup and  $MN$  is a subgroup by exercise 92. Since  $M$  and  $N$  are normal, we have  $gMg^{-1} = M$  and  $gNg^{-1} = N$  for all  $g \in G$ . Let  $x \in M \cap N$ , then  $g x g^{-1} \in M$  and  $g x g^{-1} \in N$  so  $g x g^{-1} \in M \cap N$  and thus  $g(M \cap N)g^{-1} \subseteq M \cap N$ . Replacing  $g$  by  $g^{-1}$  in the above expression shows  $g^{-1}(M \cap N)g \subseteq M \cap N$ . It follows from both of these containments that  $g(M \cap N)g^{-1} = M \cap N$  so  $M \cap N$  is a normal subgroup. Similarly  $gMNg^{-1} = (gMg^{-1})(gNg^{-1}) = MN$  for all  $g \in G$ , so  $MN$  is a normal subgroup.

- 94.** Let  $H$  and  $K$  be subgroups of a group  $G$ .

(i) If  $H \subseteq N_G(K)$  show that  $HK = KH$ .

(ii) If  $HK$  contains the inverse of each of its elements, show that  $HK = KH$ .

*Solution.*

- 95.** Let  $F$  be the free group with generators  $x$  and  $y$ . If  $G$  is an abelian group and if  $\phi: F \rightarrow G$  is a homomorphism, show that  $u^{-1}v^{-1}uv \in \ker(\phi)$  for all words  $u, v \in F$ .

- 96.** Suppose that  $H$  is the only subgroup of order  $|H|$  in the group  $G$ . Show that  $H$  is normal in  $G$ .



(b) This is a coset of the stabilizer:  $\{(1, 2, 3), (1, 2, 4), (1, 2)(3, 4)\}$ .

(c)  $\{(1, 3, 2), (1, 3, 4), (1, 3)(2, 4)\}$

(d)  $\{(1, 4, 2), (1, 4, 3), (1, 4)(2, 3)\}$

(iv) If  $a$  has order 3 and  $b$  has order 2, then the order of  $ab$  is 4. (Can you convince yourself of this fact geometrically?) Hence the order of  $|\langle a, b \rangle|$  is by Lagrange's theorem a multiple of both 3 and 4. Hence  $|\langle a, b \rangle| = 12$  and  $\langle a, b \rangle = G$ . Note that  $G$  is isomorphic to  $A_4$ .

**99.** Let  $G$  be the group of rotations of the cube  $\{x_1, x_2, x_3 \mid x_1, x_2, x_3 \in \{-1, 1\}\}$ .

(i) Label the four diagonals of the cube with the numbers 1, 2, 3 and 4. For each  $g \in G$ , let  $\phi(g)$  denote the corresponding permutation of  $\{1, 2, 3, 4\}$ . Show that  $\phi$  is an isomorphism from  $G$  onto  $S_4$ .

(ii) Label the three lines joining the centers of opposite faces with the numbers 1, 2 and 3. For each  $g \in G$ , let  $f(g)$  be the corresponding permutation of  $\{1, 2, 3\}$ . Show that the map

$$f : G \rightarrow S_3 : g \mapsto f(g)$$

is a homomorphism, and describe its kernel and image.

**100.** For each of the following subgroups of  $S_4$  find the orbits of the action on  $\{1, 2, 3, 4\}$ , and the stabilizer of each point:

(i)  $H = \langle (1, 2, 3) \rangle$ ,

(ii)  $K = \langle (1, 2)(3, 4) \rangle$ ,

(iii)  $L = A_4$ .

*Solution.*

(i) Now  $H * 1 = H * 2 = H * 3 = \{1, 2, 3\}$  and  $H * 4 = \{4\}$ . Also  $H_1 = H_2 = H_3 = \{1\}$  and  $H_4 = H$ .

(ii)  $K * 1 = K * 2 = \{1, 2\}$ ,  $K * 3 = K * 4 = \{3, 4\}$ ,  $K_1 = K_2 = K_3 = K_4 = \{1\}$ .

$$L_3 = \langle (1, 2, 4) \rangle$$

$$L_2 = \langle (1, 3, 4) \rangle$$

$$L_1 = \langle (2, 3, 4) \rangle$$

Note that the subgroups  $L_i$  are all conjugate.

**101.** We define an action of the additive group  $\mathbb{R}^+$  of real numbers on the set  $X = \mathbb{C}$  of complex numbers by

$$\theta * z = e^{i\theta} z, \text{ where } \theta \in \mathbb{R} \text{ and } z \in \mathbb{C}.$$

Describe the orbits of  $\mathbb{R}^+$  on  $X$  and the stabilizers of 0 and  $i$ .

*Solution.*

The orbits are circles  $\{z \in \mathbb{C} \mid |z| = r\}$ , centered at 0 and radius  $r$ , where  $r \geq 0$ . Also  $\text{Stab}(0) = \mathbb{R}$  and  $\text{Stab}(i) = 2\pi\mathbb{Z}$ .

**102.** If  $G$  acts on a set  $X$ , then show that the stabilizer

$$\text{Stab}_G(x) = \{g \in G \mid g * x = x\}$$

of the element  $x$ , is a subgroup.

*Solution.*

Now  $e \in \text{Stab}_G(x)$  as  $e * x = x$ . Let  $g_1, g_2 \in \text{Stab}_G(x)$ . Then  $g_1 * x = g_2 * x = x$ , so  $(g_1 g_2) * x = g_1 * (g_2 * x) = g_1 * x = x$  and  $g_1 g_2 \in \text{Stab}_G(x)$ . Also  $g_1 * x = x$  implies  $g_1^{-1} * (g_1 * x) = g_1^{-1} * x$  or  $x = g_1^{-1} * x$ , so  $g_1^{-1} \in \text{Stab}_G(x)$ . Hence  $\text{Stab}_G(x) \leq G$ .

**103.** Let  $G$  act on a set  $X$ . If the orbits  $\text{orb}_G(x_1)$  and  $\text{orb}_G(x_2)$  intersect, then show that  $\text{orb}_G(x_1) = \text{orb}_G(x_2)$ . (Hence it follows that  $X$  is partitioned into orbits.)

*Solution.*

Let  $y \in \text{orb}_G(x_1) \cap \text{orb}_G(x_2)$ . Then there exist  $g_1, g_2 \in G$  such that  $y = g_1 * x_1$  and  $y = g_2 * x_2$ . Therefore

$$\begin{aligned} \text{orb}_G(x_1) &= G * x_1 = G * (g_1^{-1} * y) = (G g_1^{-1}) * y = G * y \\ &= G * (g_2 * x_2) = (G g_2) * x_2 = G * x_2 = \text{orb}_G(x_2). \end{aligned}$$

*Solution.*

If  $h \in \text{Stab}(x)$ , then  $h(x) = x$  and so

$$(ghg^{-1})(gx) = (gh)(g^{-1}gx) = gh(x) = g(h(x)) = gx.$$

Hence  $g\text{Stab}(x)g^{-1} \subseteq \text{Stab}(gx)$ . Conversely, let  $k \in \text{Stab}(gx)$ . Then

$$(g^{-1}kg)(x) = g^{-1}(k(gx)) = g^{-1}(gx) = x.$$

Hence  $g^{-1}\text{Stab}(gx)g \subseteq \text{Stab}(x)$  and so  $g\text{Stab}(x)g^{-1} \subseteq \text{Stab}(gx)$ . As each set contains the other, it follows that  $g\text{Stab}(x)g^{-1} = \text{Stab}(gx)$ .

**105.** Let  $G$  acts on the set  $X$ . If  $g \in G$  and  $x \in X$  show that  $\text{fix}(ghg^{-1}) = g\text{fix}(h)$ . (Recall that  $\text{fix}(h) = \{x \in X \mid h * x = x\}$ .)

*Solution.*

Let  $x \in g\text{fix}(h)$ , then  $g^{-1} * x \in \text{fix}(h)$  so  $h * g^{-1}x = g^{-1}x$ . This last equation may be written  $ghg^{-1} * x = x$  i.e.  $x \in \text{fix}(ghg^{-1})$ . Conversely, suppose that  $x \in \text{fix}(ghg^{-1})$ , then  $ghg^{-1} * x = x$  and so  $h * g^{-1}x = g^{-1}x$ . This last equation states  $x \in g\text{fix}(h)$ .

**106.** Let  $H$  be a subgroup of the group  $G$  and define an action of  $H$  on  $G$  by

$$h * x = hx, \text{ where } h \in H \text{ and } x \in G,$$

that is  $H$  acts via multiplication on the left. Show that the orbits are the right cosets of  $H$  in  $G$ .

*Solution.*

Note that  $H$  acts on  $G$  since

$$h_1 * (h_2 * x) = h_1(h_2x) = (h_1h_2)x = (h_1h_2) * x.$$

By definition  $\text{orb}_H(x) = \{h * x \mid h \in H\} = Hx$ , and the stablizer of any element  $x$  is the trivial subgroup.

$$L(g) : xH \mapsto gxH.$$

- (i) Show that  $L(g)$  is a permutation of  $X$ .
- (ii) Show that  $L : G \rightarrow \text{Sym}(X) \mid g \mapsto L(g)$  is a homomorphism into the symmetric group  $\text{Sym}(X)$ .
- (iii) Show that  $\ker(L) = \bigcap_{x \in G} xHx^{-1}$ .
- \*(iv) Show that  $\ker(L)$  is the largest normal subgroup of  $G$  that is contained in  $H$ .

*Solution.*

The proof of this exercise is almost identical to the proof of Cayley's theorem. Indeed, it is the same result if  $H$  is the trivial subgroup.

- (i) Now  $L(g) \circ L(g^{-1}) = \iota_X$  and  $L(g^{-1}) \circ L(g) = \iota_X$  so  $L(g)$  is invertible and so is an element of  $\text{Sym}(X)$ .
- (ii) We show that  $L(g_1) \circ L(g_2) = L(g_1g_2)$  by showing that the functions have the same effect on the elements of  $X$ . Note that

$$L(g_1) \circ L(g_2)(xH) = L(g_1)(g_2xH) = g_1g_2xH = L(g_1g_2)(xH).$$

- (iii) Now  $g \in \ker(L)$  iff  $L(g)$  is the identity permutation iff  $L(g)(xH) = gxH = xH$  for all  $x \in G$ . Hence  $g \in xHx^{-1}$  for all  $x \in G$ , and so  $\ker(L) \subseteq \bigcap_{x \in G} xHx^{-1}$ . The reverse containment can be seen by reversing this argument.
- (iv) Now  $\bigcap_{x \in G} xHx^{-1}$  is a normal subgroup of  $G$  contained in  $H$ . If  $N$  were a normal subgroup of  $G$  contained in  $H$ , then  $N \subseteq xHx^{-1}$  for all  $x \in G$ . Hence  $N \subseteq \bigcap_{x \in G} xHx^{-1}$ .

**108.** If  $H$  and  $K$  are subgroups of  $G$  of finite index show that  $H \cap K$  is also a subgroup of finite index.

*Solution.*

Suppose that

$$G = Hx_1 \sqcup \cdots \sqcup Hx_m \text{ and } G = Ky_1 \sqcup \cdots \sqcup Ky_n$$

Hence

$$Hx_i = Hx_i \cap G = (Hx_i \cap Ky_1) \sqcup \cdots \sqcup (Hx_i \cap Ky_n)$$

is a union of at most  $n$  cosets of  $H \cap K$ . Hence  $|G : H \cap K| \leq mn$  is finite.

**109.** Suppose that  $G$  acts on a set  $X$  and that  $H$  is a subgroup of  $G$ . If  $x \in X$  show that  $\text{orb}_G(x) = \text{orb}_H(x)$  if and only if  $G = H\text{Stab}_G(x)$ .

*Solution.*

Suppose that  $G = H\text{Stab}_G(x)$ , then

$$\text{orb}_G(x) = G * x = (H\text{Stab}_G(x)) * x = H(\text{Stab}_G(x) * x) = H * x = \text{orb}_H(x).$$

Conversely, suppose that  $\text{orb}_G(x) = \text{orb}_H(x)$ . Let  $g \in G$ . Then  $g * x \in \text{orb}_H(x)$  so there exists an  $h \in H$  such that  $g * x = h * x$ . Therefore  $h^{-1}g * x = x$  so  $h^{-1}g \in \text{Stab}_G(x)$ . Therefore,  $G \subseteq H\text{Stab}_G(x)$  and so equality follows.

**110.** If  $N$  is normal in  $G$  and  $G/N$  contains a subgroup of index 2, show that  $G$  has a subgroup of index 2 which contains  $N$ .

*Solution.*

Let  $\phi : G \rightarrow G/N : x \mapsto xN$  and let  $H^*$  be a subgroup of  $G/N$  of index 2. By the correspondence theorem  $\phi^{-1}(H^*)$  is a subgroup of index 2 in  $G$  containing  $N$ .

**111.** Show that there are only two different groups of order 6.

*Solution.*

Let  $G$  be a group of order 6. By Cayley's theorem there are elements  $h$  and  $k$  of orders 2 and 3 respectively. By exercise 90 the subgroup  $K = \langle k \rangle$  of index 2 is normal in  $G$ . Hence  $hkh^{-1} \in K$ . There are two possibilities. Either  $hkh^{-1} = k$  or  $hkh^{-1} = k^{-1}$ . In the first case  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ , while in the second case,  $G \cong D_6 \cong S_3$ .

**112.** Prove that the only noncyclic group of order 4 is  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

*Solution.*

Let  $G$  be an element of order 4. By Lagrange's theorem, the order of an element of  $G$  is 1, 2 or 4. If there is an element of order 4, then  $G$  is isomorphic to  $\mathbb{Z}_4$ . If every element has order 1 or 2, then  $x^2 = e$  for all  $x \in G$ , so it follows that  $G$  is abelian. Hence  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ .

- (ii) If  $x \in A_n$ , what is the relationship between the conjugates of  $x$  in  $A_n$  and the conjugates of  $x$  considered as an element of  $S_n$ ?

*Solution.*

- (i) Let  $C = C_{S_n}(x)$ . Suppose that  $C$  is not a subset of  $A_n$ . Then  $S_n = CA_n$  and so by the second isomorphism theorem

$$\mathbb{Z}_2 \cong S_n/A_n = CA_n/A_n \cong C/(C \cap A_n).$$

Since  $C \cap A_n = C_{A_n}(x)$ , we have  $|C_{A_n}(x)| = \frac{1}{2}|C_{S_n}(x)|$ .

- (ii) By the previous part, the  $S_n$ -conjugacy class of  $x$  either equals the  $A_n$ -conjugacy class of  $x$  or it splits into two  $A_n$ -conjugacy classes. (The latter happens, by the way, if  $x$  is a product of disjoint cycles of distinct odd length. We are counting one-cycles for this criterion. Thus, for example,  $(1, 2, 3, 4, 5)(6, 7, 8)(9)$  is a possibility in  $S_9$ , but not in  $S_{10}$ .)

- 114.** Let  $G$  be a group. If the conjugacy class of  $x \in G$  contains precisely two elements, show that  $G$  is not a simple group. (Note that the index of the centralizer  $C_G(x)$  in  $G$  equals the size of the conjugacy class containing  $x$ .)

*Solution.*

Since  $|G : C_G(x)| = 2$ ,  $C_G(x)$  is a subgroup of index two in  $G$  and hence is normal. If  $C_G(x)$  is the trivial subgroup, then  $x = e$  as  $x \in C_G(x)$ . This is not possible as the conjugacy class containing identity element has only one element and not 2. Therefore  $C_G(x)$  is a proper nontrivial subgroup of  $G$ . Hence  $G$  is not simple.

- 115.** Find the conjugacy classes of  $S_6$  and  $A_6$ . Show that  $A_6$  is a simple group.

- 116.** For each  $x \in \{e, (1, 2), (1, 2, 3), (1, 2, 3, 4), (1, 2)(3, 4)\}$  compute the centralizer in  $S_4$  of  $x$ .

*Solution.*

There are two ways to do this question. One way is a simple-minded use of the substitution rule (backwards) to solve for all  $y \in S_4$  which centralize the given element. This works but gives little insight and is hard when the centralizer is large. Another approach is to calculate  $|C_{S_4}(x)|$  and thereby determine generators

$$\begin{aligned}
C_{S_4}((1, 2)) &= \langle (1, 2), (3, 4) \rangle, \\
C_{S_4}((1, 2, 3)) &= \langle (1, 2, 3) \rangle, \\
C_{S_4}((1, 2, 3, 4)) &= \langle (1, 2, 3, 4) \rangle, \\
C_{S_4}((1, 2)(3, 4)) &= \langle (1, 2), (1, 3, 2, 4) \rangle
\end{aligned}$$

**117.** If  $G = S_4$  and  $H = \langle (1, 2, 3, 4) \rangle$ , then compute  $N_G(H)$ .

*Solution.*

Now  $|G : N_G(H)|$  is the number of conjugates of  $H$  in  $G$ . There are 6 conjugates of the *element*  $(1, 2, 3, 4)$  in  $G$ . Some of these conjugates generate the same cyclic group. For example,  $\langle (1, 2, 3, 4) \rangle = \langle (1, 4, 3, 2) \rangle$ . Indeed, there are 3 conjugates of the *subgroup*  $H = \langle (1, 2, 3, 4) \rangle$  in  $G$ . Hence  $|N_G(H)| = \frac{4!}{3} = 8$ . Now  $x = (1, 4)(2, 3)$  conjugates  $(1, 2, 3, 4)$  to its inverse and so normalizes  $H$ . Since  $x \notin H$ , the subgroup  $\langle x, H \rangle$  has order 8 and normalizes  $H$ . Thus  $N_G(H) = \langle (1, 2, 3, 4), (1, 4)(2, 3) \rangle$ .

In general, if  $|x| = n$ , then  $x$  and  $x^k$  have the same disjoint cycle structure iff  $\gcd(k, n) = 1$ . By the substitution rule,  $x$  and  $x^k$  are conjugate and one may show that

$$N_{S_n}(\langle x \rangle) / \langle x \rangle \cong \mathbf{Z}_n^\times.$$

**118.** Find all the Sylow 2-subgroups of  $S_4$ .

*Solution.*

A Sylow 2-subgroup of  $S_4$  has order 8. Therefore  $P = \langle (1, 2, 3, 4), (1, 4)(2, 3) \rangle$  is a Sylow 2-subgroup. The others are all conjugates of  $P$ . Suppose there are  $n_2$  Sylow 2-subgroups. By Sylow's third theorem  $n_2 \equiv 1 \pmod{2}$  and  $n_2 | 3$ . Thus  $n_2 = 1, 3$ . Since  $P$  is not normal in  $S_4$ ,  $n_2 = 3$ . Indeed, the Sylow 2-subgroups are

$$P, (1, 2, 3)P(1, 2, 3)^{-1} \text{ and } (1, 2, 3)^2P(1, 2, 3)^{-2}.$$

**119.** Let  $P$  be a  $p$ -subgroup of  $G$ , where  $p$  is a prime, and let  $N$  be a normal subgroup of  $G$ . Show that  $P \cap N$  is a  $p$ -subgroup of  $N$ . In addition, show that  $p$  divides  $|N : P \cap N|$  implies that  $p$  divides  $|G : P|$ .

*Solution.*

Now  $|NP : P \cap N| = |NP : P| \cdot |P : P \cap N| = |NP : N| \cdot |N : P \cap N|$  and by the second isomorphism theorem  $|NP : N| = |P : P \cap N|$ , hence  $|NP : P| = |N : P \cap N|$ . Therefore  $p$  divides  $|N : P \cap N|$  implies  $p$  divides  $|NP : P|$ , which in turn divides  $|G : P|$ .

*Solution.*

We have proved earlier that the product of normal subgroups is a normal subgroup. If  $M_1$  and  $M_2$  are  $p$ -subgroups, then so is  $M_1 \cap M_2$ . It follows from the equation  $|M_1 M_2| \cdot |M_1 \cap M_2| = |M_1| \cdot |M_2|$  (which follows from the second isomorphism theorem) that  $|M_1 M_2|$  is a power of  $p$ . Hence  $|M_1 M_2|$  is a normal  $p$ -subgroup. The product of all the normal  $p$ -subgroups of a finite group  $G$  (there are finitely many of course) is therefore a normal  $p$ -subgroup of  $G$ .

**121.** If  $N$  is a subgroup of  $Z(G) = \{z \in G \mid gz = zg \text{ for all } g \in G\}$ , prove that  $N$  is a normal subgroup of  $G$ .

*Solution.*

It is clear from the definition of  $Z(G)$  that  $gZ(G) = Z(G)g$  for all  $g \in G$ . Hence  $Z(G) \trianglelefteq G$ . Note that  $Z(G) = G$  iff  $G$  is abelian. Also  $Z(G)$  is the kernel of the homomorphism

$$\rho: G \rightarrow \text{Aut}(G): g \mapsto \rho(g)$$

where  $\rho(g)$  is the inner automorphism  $G \rightarrow G: x \mapsto gxg^{-1}$ .

**122.** Let  $U(2)$  denote the group of all  $2 \times 2$  matrices  $A$  with complex entries which satisfy  $A\bar{A}^t = I$ .

(i) Show that each element of  $U(2)$  can be written in the form

$$\begin{pmatrix} a & b \\ -\Delta\bar{b} & \Delta\bar{a} \end{pmatrix},$$

where  $a, b$  and  $\Delta$  are complex numbers such that  $a\bar{a} + b\bar{b} = 1$  and  $\Delta\bar{\Delta} = 1$ .

(ii) Show that the map  $\phi: U(2) \rightarrow \mathbf{C}^\times$  defined by  $A \mapsto \det(A)$  is a homomorphism. The kernel of  $\phi$  is called the *special unitary group*  $SU(2)$ .

**\*123.** Let  $O(3)$  be the group of all  $3 \times 3$  real matrices  $X$  such that  $XX^t = I$ . (This is called the *orthogonal group*.) Define the function  $\phi: SU(2) \rightarrow O(3)$  by

$$\phi(A) = \begin{pmatrix} \frac{1}{2}(a^2 + \bar{a}^2 - b^2 - \bar{b}^2) & \frac{1}{2}i(a^2 - \bar{a}^2 + b^2 - \bar{b}^2) & \bar{a}b + ab \\ \frac{1}{2}i(-a^2 + \bar{a}^2 + b^2 - \bar{b}^2) & \frac{1}{2}(a^2 + \bar{a}^2 + b^2 + \bar{b}^2) & i(\bar{a}b - ab) \\ -(\bar{a}b + a\bar{b}) & i(\bar{a}b - a\bar{b}) & a\bar{a} - b\bar{b} \end{pmatrix}$$

where  $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ . Show that  $\phi$  is a homomorphism whose kernel is  $\{-I, I\}$ .

*Solution.*

Now  $n_3|4$  and  $n_3 \equiv 1 \pmod{4}$ , so  $n_3 = 1, 4$ . If  $n_3 = 1$ , then  $G$  has a normal Sylow 3-subgroup  $P$ , and so using the correspondence theorem  $G/P$  has a subgroup of index 2 – a contradiction. Thus  $n_3 = 4$  and there is a nontrivial homomorphism  $\phi: G \rightarrow S_4$  induced by conjugation on the 4 Sylow 3-subgroups. Suppose that  $x \in \ker(\phi)$  and  $P_1, P_2, P_3, P_4$  are the Sylow 3-subgroups. Then  $x \in N_G(P_i)$ ,  $1 \leq i \leq 4$ . But  $N_G(P_i) = P_i$  so  $\ker(\phi) = \{e\}$ . Hence  $\phi$  is injective and  $G \cong \phi(G) = A_4$ .

**\*125.** If  $G$  is a group of order  $2m$ , where  $m$  is odd, show that  $G$  has a (normal) subgroup of index 2.

*Solution.*

By Cayley's theorem there is an injective homomorphism  $L: G \rightarrow \text{Sym}(G)$ . By Cauchy's theorem there is an element  $g \in G$  of order 2. The disjoint cycle decomposition of  $L(g)$  is a product of  $m$  disjoint transpositions. Hence  $L(g)$  is odd and so  $A_{2m}L(G) = S_{2m}$ . By the second isomorphism theorem

$$\mathbb{Z}_2 \cong S_{2m}/A_{2m} = A_{2m}L(G)/A_{2m} \cong L(G)/(A_{2m} \cap L(G)).$$

Hence  $A_{2m} \cap L(G)$  is a subgroup of  $L(G)$  of index 2. By the correspondence theorem,  $G$  has a subgroup of index 2, namely  $L^{-1}(A_{2m} \cap L(G))$ .

**126.** Let  $x$  be an element of a group  $G$ , and suppose that  $|x| = m_1m_2$  where  $m_1$  and  $m_2$  have no common factors. Show that there exist  $x_1, x_2 \in G$  such that  $x = x_1x_2 = x_2x_1$  where  $|x_1| = m_1$  and  $|x_2| = m_2$ . Furthermore, if  $x = y_1y_2 = y_2y_1$  where  $|y_1| = m_1$  and  $|y_2| = m_2$ , show that  $x_1 = y_1$  and  $x_2 = y_2$ .

*Solution.*

Since  $\gcd(m_1, m_2) = 1$ , there exist integers  $M_1$  and  $M_2$  such that  $M_1m_1 + M_2m_2 = 1$ . Therefore,

$$x = x^1 = x^{M_1m_1 + M_2m_2} = x^{M_1m_1}x^{M_2m_2}.$$

The order of  $x^{m_1}$  is  $m_2$  and since  $\gcd(m_1, M_1) = 1$ ,  $x_2 = x^{m_1M_1}$  has the same order. Similarly,  $x_1 = x^{m_2M_2}$  has order  $m_1$ . Since both  $x_1$  and  $x_2$  are powers of  $x$ , we have  $x_1x_2 = x_2x_1$ . Suppose now that  $x = y_1y_2 = y_2y_1$  where  $|y_1| = m_1$  and  $|y_2| = m_2$ . Since  $y_1^{m_1} = y_2^{m_2} = 1$  we have

$$x^{m_1M_1} = (y_1y_2)^{m_1M_1} = y_1^{m_1M_1}y_2^{m_1M_1} = y_2^{1-m_2M_2} = y_2.$$

Similarly,  $y_1 = x^{m_2M_2}$ .

*Solution.*

Let  $r = |G : N_G(H)|$  and let  $H_1, \dots, H_r$  be the  $r$  distinct conjugates of  $H$ . Suppose  $G = H_1 \cup \dots \cup H_r$ . Since  $|H_i| = |H|$ , we have

$$|G| \leq |H_1| + \dots + |H_r| = r|H|.$$

However,  $r|H| \leq r|N_G(H)| = |G : N_G(H)| \cdot |N_G(H)| = |G|$ . Hence  $G = H_1 \sqcup \dots \sqcup H_r$  is a disjoint union. This is a contradiction, as the identity element is common to all the  $H_i$ .

**128.** Show that the smallest nonabelian simple group is  $A_5$ .

*Solution.*

Groups of orders  $p^n, pq, p^2q, pqr$  are not simple. This excludes all of the orders  $< 60$  except 48. The order 48 is easily excluded as  $n_2 = 1, 3$  and there is no nontrivial homomorphism  $G \rightarrow S_3$ .

**129.** (i) Find the order of a Sylow 2-subgroup of  $S_8$ .

\*(ii) Find the order of a Sylow 2-subgroup of  $S_{2^n}$ .

*Solution.*

Let  $|n|_2$  denote the largest power of two that divides  $n$ . It follows that  $|mn|_2 = |m|_2 |n|_2$ .

(i) The order of a Sylow 2-subgroup of  $S_8$  is  $|8!|_2 = 2^7$ .

(ii) If  $|x|_2 = 2^y$ , then a table of  $y$  versus  $x$  shows a pattern:

$$\left( \begin{array}{c|cccccccccccccccc} x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ y & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 3 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 4 \end{array} \right).$$

In particular,  $|x|_2$  equals  $|2^n + x|_2$  if  $1 \leq x < 2^n$ , and equals  $2|2^n + x|_2$  if  $x = 2^n$ . Thus by induction,

$$\begin{aligned} |2^{n+1}|_2 &= |2^n!|_2 |2^n + 1|_2 \cdots |2^n + 2^n|_2 \\ &= 2^{2^n - 1} \cdot 2^{2^n - 1} \cdot 2 && \text{by induction} \\ &= 2^{2^{n+1} - 1} \end{aligned}$$

One answer is  $\langle(1, 2, 3), (4, 5, 6)\rangle$ .

**131.** Find a Sylow 3-subgroup of  $S_9$ .

*Solution.*

One answer is  $\langle(1, 2, 3), (4, 5, 6), (7, 8, 9), (1, 4, 7)(2, 5, 8)(3, 6, 9)\rangle$ .

**132.** Suppose that  $|G| = p^n q$ , where  $p$  and  $q$  are distinct primes. Let  $Q$  be a Sylow  $q$ -subgroup and suppose that  $N_G(Q) = Q$ . Show that the Sylow  $p$ -subgroup of  $G$  is normal.

*Solution.*

The number of conjugates of  $Q$  in  $G$  is  $|G : N_G(Q)| = |G : Q| = p^n$ . If  $Q_1$  and  $Q_2$  are distinct conjugates of  $Q$ , then  $Q_1 \cap Q_2 = \{e\}$ . Hence there are  $p^n(q - 1)$  elements of  $G$  with order  $q$ , as these are precisely the nontrivial elements of the Sylow  $q$ -subgroups. There are  $p^n$  remaining elements of  $G$ . Since  $G$  has a Sylow  $p$  subgroup, it has at least  $p^n$  elements whose order is a power of  $p$ . Hence  $G$  has *precisely*  $p^n$  elements of order a power of  $p$ . Hence there is only one Sylow  $p$ -subgroup of  $G$ , and so it is normal.

**133.** Show that any group of order 42 has a normal subgroup of order 7.

*Solution.*

Since  $n_7 \equiv 1 \pmod{7}$  and  $n_7 | 6$ , it follows that  $n_7 = 1$ . Hence the Sylow 7-subgroup is normal.

**134.** If  $P$  is a Sylow  $p$ -subgroup of  $G$ , show that  $P$  is the only Sylow  $p$ -subgroup of  $N_G(P)$ . Hence, or otherwise, show that  $N_G(N_G(P)) = N_G(P)$ .

*Solution.*

Since  $P$  is contained in  $N_G(P)$ , and  $P$  is a Sylow  $p$ -subgroup of  $G$ , it follows that  $P$  is a Sylow  $p$ -subgroup of  $N_G(P)$ . If  $P'$  were another Sylow  $p$ -subgroup of  $N_G(P)$ , then by Sylow's second theorem, there is an  $x \in N_G(P)$  such that  $P' = xPx^{-1}$ . However, by definition,  $P$  is a normal subgroup of  $N_G(P)$ , so  $P = xPx^{-1} = P'$ . Suppose now that  $x \in N_G(N_G(P))$ . Since  $xPx^{-1}$  is a Sylow  $p$ -subgroup of  $N_G(P)$  and  $P$  is the only Sylow  $p$ -subgroup of  $N_G(N_G(P))$ , we see that  $xPx^{-1} = P$  so

**135.** If  $H$  and  $K$  are nontrivial subgroups of  $\mathbf{Q}^+$ , the additive group of rational numbers, show that  $H \cap K \neq \{0\}$ .

*Solution.*

Let  $\frac{h_1}{h_2} \in H$  and  $\frac{k_1}{k_2} \in K$  where  $h_1, h_2, k_1, k_2 \in \mathbf{Z}$  are all nonzero. Then  $h_1 k_1 \neq 0$  and  $h_1 k_1 = h_1 k_1 h_2 \frac{h_1}{h_2} \in H$  and  $h_1 k_1 k_2 \frac{k_1}{k_2} \in K$ . Hence  $H \cap K \neq \{0\}$ .

**136.** Give  $q$  colours, how many distinct  $3 \times 3$  chessboards are there? (Note that the group acting here is cyclic of order 4 generated by a rotation of  $2\pi/4$ . The generator may be viewed as a permutation of the  $3^2$  ordered squares and is a product of disjoint 4-cycles and a 1-cycle.)

**\*137.** Determine the number of distinct roulette wheels with  $n$  sectors which can be coloured with  $q$  different colours. First solve the cases when  $n = 7$  and  $n = 8$ .

*Solution.*

Let  $g$  be a rotation by  $2\pi/n$ . Then  $G = \langle g \rangle$  permutes the set  $X$  of  $q^n$   $n$ -sector  $q$ -colourable roulette wheels. By the Cauchy-Frobenius theorem, the number of distinct roulette wheels is

$$\frac{1}{n} \sum_{i=0}^{n-1} F(g^i)$$

where  $F(g^i)$  is the number of roulette wheels fixed by  $g^i$ . If  $n = 7$ , then  $F(e) = q^7$  as all the 7 sectors can be coloured independently, and  $F(g^i) = q$ , for  $1 \leq i \leq 6$  as a roulette wheel fixed by  $g^i$ ,  $1 \leq i \leq 6$  must have all its sectors the same colour. Thus there are  $\frac{1}{7}(q^7 + 6q)$  distinct roulette wheels. If  $n = 8$ , then  $F(e) = q^8$  and

$$\begin{aligned} F(g) &= F(g^{-1}) = q \\ F(g^2) &= F(g^{-2}) = q^2 \\ F(g^3) &= F(g^{-3}) = q \\ F(g^4) &= q^4. \end{aligned}$$

Thus there are  $\frac{1}{8}(q^8 + q^4 + 2q^2 + 4q)$  distinct roulette wheels.

In general  $g^i$  has order  $n/\gcd(i, n)$  so  $F(g^i) = q^{\gcd(i, n)}$ . Thus there are

$$\frac{1}{n} \sum_{i=0}^{n-1} q^{\gcd(i, n)}$$

where  $d$  ranges over the (positive) divisors of  $n$ .

- 138.** How many distinguishable ways can the faces of a regular tetrahedron be coloured with  $q$  different colours? (The group acting here is the group of 12 rotations of the tetrahedron. These may be identified with the elements of  $A_4$  as each symmetry of the tetrahedron gives rise to a permutation of the four faces.)

*Solution.*

The group of rotations of a regular tetrahedron may be identified with  $A_4$  by considering permutations of the 4 vertices of the tetrahedron. For this exercise, however, it is more fruitful to view the group of rotations as a permutation group on the four faces of the tetrahedron. If  $g, h \in A_4$  are conjugate, then by exercise 105,  $F(g) = F(h)$ . Hence the Cauchy-Frobenius theorem states that the number of orbits of the action of  $G$  on  $X$  is

$$\frac{1}{|G|} \sum |G : C_G(g)| \cdot F(g)$$

where the sum ranges over representatives from each conjugacy class of  $G = A_4$ . Now  $F(\iota) = q^4$ ,  $F((1, 2, 3)) = q^2$ ,  $F((1, 3, 2)) = q^2$  and  $F((1, 2)(3, 4)) = q^2$ . Note that  $\iota$ ,  $(1, 2, 3)$ , and  $(1, 2)(3, 4)$  have 4, 2 and 2 orbits when acting on the set  $\{1, 2, 3, 4\}$ . By the Cauchy-Frobenius theorem, the number of distinct coloured tetrahedra is

$$\frac{1}{12}(q^4 + 4q^2 + 4q^2 + 3q^2) = \frac{q^2}{12}(q^2 + 11).$$