$C = \{5, 6, 7\}$. By considering A^{-1} and B^{-1}, solve the two equations $A \Delta X = B$, and $A \Delta X \Delta B = C$.

1.3 Permutations of a finite set

We shall now discuss permutations of a non-empty set X. We shall show (in Section 1.5) that the permutations of X form a group, and we shall use this to examine the nature of the permutations. This is most effective when X is a finite set, and we shall assume that this is so during this and the next section. Before we can consider permutations we need to understand what we mean by a function and, when it exists, its inverse function. As (for the moment) we are only considering functions between finite sets, we can afford to take a fairly relaxed view about functions; a more detailed discussion of functions (between arbitrary sets) is given in Section 1.5.

A *function* $f : X \to X$ from a finite set X to itself is a rule which assigns to each x in X a unique element, which we write as $f(x)$, of X. We can define such a function by giving the rule explicitly; for example, when $X = \{a, b, c\}$ we can define $f : X \to X$ by the rule $f(a) = b$, $f(b) = c$ and $f(c) = a$. Note that f cyclically permutes the elements a, b and c, and this is our first example of a permutation. Two functions, say $f : X \to X$ and $g : X \to X$ are *equal* if $f(x) = g(x)$ for every x in X, and in this case we write $f = g$. The *identity function* $I : X \to X$ on X is the function given by the rule $I(x) = x$ for all x in X.

Suppose now that we have two functions f and g from X to itself. Then for every x in X there is a unique element $g(x)$ in X, and for every y in X there is a unique element $f(y)$ in X. If we choose x first, and then take $y = g(x)$, we have created a rule which takes us from x to the element $f(g(x))$. This rule defines a function which we denote by $fg : X \to X$. We call this function the *composition* (or sometimes the *product*) of f and g, and it is obtained by *applying g first, and then f*. This function is sometimes denoted by $f \circ g$, but it is usual to use the less cumbersome notation fg.

Given a function $f : X \to X$, the function $g : X \to X$ is the *inverse* of f if, for every x in X, we have $f(g(x)) = x$ and $g(f(x)) = x$, or, more succinctly, if $fg = I = gf$, where I is the identity function on X. It is important to note that not every function $f : X \to X$ has an inverse function. Indeed, *f has an inverse function precisely when, for every y in X, there is exactly one x in X such that $f(x) = y$*, for then the inverse function is the rule which takes y back to x. We say that a function $f : X \to X$ is *invertible* when the inverse of f exists, and then we denote the inverse by f^{-1}. Note that if f is invertible, then so is f^{-1}, and $(f^{-1})^{-1} = f$. We are now ready to define what we mean by a permutation of a set X.

Definition 1.3.1 A *permutation* of X is an invertible map $f : X \to X$. The set of permutations of X is denoted by $\mathcal{P}(X)$. □

Theorem 1.3.2 *The set $\mathcal{P}(X)$ of permutations of a finite non-empty set X is a group with respect to the composition of functions.*

We remark that it is usual to speak of the *product of permutations* rather than the composition of permutations.

Proof We must show that the operation $*$ defined on $\mathcal{P}(X)$ by $f * g = fg$ (the composition) satisfies the requirements of Definition 1.2.1. First, we show that $*$ is associative. Let f, g and h be any functions, and let $u = gf$ and $v = hg$. Then, for every x in X,

$$\begin{aligned} \big(h(gf)\big)(x) &= \big(hu\big)(x) \\ &= h\big(u(x)\big) \\ &= h\Big(g\big(f(x)\big)\Big) \\ &= v\big(f(x)\big) \\ &= (vf)(x) \\ &= \big((hg)f\big)(x). \end{aligned} \tag{1.3.1}$$

This shows that $h(gf) = (hg)f$ and, as a consequence of this, we can now use the notation hgf (without brackets) for the composition of three (or more) functions in an unambiguous way.

Next, the identity map $I : X \to X$ is the identity element of $\mathcal{P}(X)$ because if f is any permutation of X, then $fI = f = If$; explicitly, for every x, $fI(x) = f(x) = I(f(x))$. Next, if f is any permutation of X, then f is invertible, and the inverse function f^{-1} is also a permutation of X (because it too is invertible). Moreover, f^{-1} is the inverse of f in the sense of groups because $ff^{-1} = I = f^{-1}f$. Finally, suppose that f and g are permutations of X. Then fg is invertible (and so is a permutation of X) with inverse $g^{-1}f^{-1}$; indeed

$$(fg)(g^{-1}f^{-1}) = f(gg^{-1})f^{-1} = fIf^{-1} = ff^{-1} = I,$$

and similarly, $(g^{-1}f^{-1})(fg) = I$. This completes the proof. □

Examples of permutation groups will occur throughout this text. However, for the rest of this and the next section we shall focus on the group of permutations of the finite set $\{1, 2, \ldots, n\}$ of integers.

Definition 1.3.3 The *symmetric group* S_n is the group of permutations of $\{1, \ldots, n\}$. □

As a permutation ρ is a function we can use the usual notation $\rho(k)$ for the image of an integer k under ρ. However, it is customary, and convenient, to write ρ in the form

$$\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix},$$

where the image $\rho(k)$ of k is placed in the second row underneath k in the first row; for example, the permutation β of $\{1, 2, 3, 4\}$ such that $\beta(1) = 4$, $\beta(2) = 2$, $\beta(3) = 1$ and $\beta(4) = 3$ is denoted by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

It is not necessary to order the columns according to the natural order of the top row, and we may use any order that we wish; for example,

$$\rho = \begin{pmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{pmatrix}, \quad \rho^{-1} = \begin{pmatrix} a_1 & \cdots & a_n \\ 1 & \cdots & n \end{pmatrix}.$$

A permutation ρ is said to *fix* k, and k is a *fixed point* of ρ, if $\rho(k) = k$. By convention, we may omit any integers in the expression for ρ that are fixed by ρ (and any integers that are omitted in this expression may be assumed to be fixed by ρ). For example, if ρ is a permutation of $\{1, \ldots, 9\}$, and if

$$\rho = \begin{pmatrix} 1 & 8 & 3 & 7 \\ 8 & 1 & 7 & 3 \end{pmatrix},$$

then ρ interchanges 1 and 8, and 3 and 7, and it fixes 2, 4, 5, 6 and 9.

If α and β are permutations of $\{1, \ldots, n\}$ then $\alpha\beta$ is the permutation obtained by applying β first and then α. The following simple example illustrates a purely mechanical way of computing this composition: if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

then (re-arranging α so that its top row coincides with the bottom row of β, and remembering that we apply β first) we have

$$\alpha\beta = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Note that $\alpha\beta \neq \beta\alpha$ (that is, α and β do not commute). We shall now define what we mean by disjoint permutations, and then show that *disjoint permutations commute*.

Definition 1.3.4 We say that two permutations α and β are *disjoint* if, for every k in $\{1, \ldots, n\}$, either $\alpha(k) = k$ or $\beta(k) = k$. □

Theorem 1.3.5 *If α and β are disjoint permutations then $\alpha\beta = \beta\alpha$.*

Proof Take any k in $\{1, \ldots, n\}$. As either α or β fixes k we may suppose that $\alpha(k) = k$. Let $k' = \beta(k)$; then $\alpha(\beta(k)) = \alpha(k')$ and $\beta(\alpha(k)) = \beta(k) = k'$ so we need to show that α fixes k'. This is true (by assumption) if β does not fix k', so we may suppose that β fixes k'. But then $\beta(k) = k' = \beta(k')$, and applying β^{-1}, we see that $k = k'$, so again α fixes k'. □

A permutation that cyclically permutes some set of integers is called a cycle. More precisely, we have the following definition.

Definition 1.3.6 The *cycle* $(n_1 \ \ldots \ n_q)$ is the permutation

$$\begin{pmatrix} n_1 & n_2 & \cdots & n_{q-1} & n_q \\ n_2 & n_3 & \cdots & n_q & n_1 \end{pmatrix}.$$

Explicitly, this maps n_j to n_{j+1} when $1 \leq j < q$, and n_q to n_1, and it fixes all other integers in $\{1, \ldots, n\}$. We say that this cycle has *length* q, or that it is a *q-cycle*. □

Notice that we can write a cycle in three different ways; for example,

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

To motivate the discussion that follows, observe that if

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

then (by inspection) $\sigma = (1\,5\,4)(2\,7\,6\,3)$ and so, by Theorem 1.3.5,

$$\sigma = (1\,5\,4)(2\,7\,6\,3) = (2\,7\,6\,3)(1\,5\,4).$$

We shall now show that this is typical of *all* permutations. Take any permutation ρ of $\{1, \ldots, n\}$, and any integer k in this set. By applying ρ repeatedly we obtain the points k, $\rho(k)$, $\rho^2(k)$, ..., and as two of these points must coincide, we see that there are integers p and q with $\rho^p(k) = \rho^q(k)$ where, say, $q < p$. As ρ^{-1} exists, $\rho^{p-q}(k) = k$. Now let u be the smallest positive integer with the property that $\rho^u(k) = k$; then the distinct numbers k, $\rho(k)$, $\rho^2(k)$, ..., $\rho^{u-1}(k)$ are cyclically permuted by ρ. We call

$$O(k) = \{k, \rho(k), \rho^2(k), \ldots, \rho^{u-1}(k)\}. \tag{1.3.2}$$

the *orbit* of k under ρ. Now every point m in $\{1, \ldots, n\}$ lies in some orbit (which will have exactly one element if and only if ρ fixes m), and it is evident that

two orbits are either identical or disjoint. Thus we can write

$$\{1, \ldots, n\} = O(k_1) \cup \cdots \cup O(k_m), \tag{1.3.3}$$

where the orbits $O(k_i)$ are pairwise disjoint sets, and where each of these sets is cyclically permuted by ρ. We call (1.3.3) the *orbit-decomposition* of $\{1, \ldots, n\}$.

Each orbit $O(k)$ in (1.3.2) provides us with an associated cycle

$$\rho_0 = (k\ \rho(k)\ \rho^2(k)\ \cdots\ \rho^{u-1}(k)).$$

Note that ρ and ρ_0 have exactly the same effect on the integers in $O(k)$, but that ρ_0 fixes every integer that is not in $O(k)$. Now consider the decomposition (1.3.3) of $\{1, \ldots, n\}$ into mutually disjoint orbits, and let ρ_j be the cycle associated to the orbit $O(k_j)$. Then it is clear that the cycles ρ_j are pairwise disjoint (because their corresponding orbits are); thus they commute with each other. Finally, if $x \in O_j$, then $\rho_j(x) = \rho(x)$, and $\rho_i(x) = x$ if $i \neq j$, so that $\rho = \rho_1 \cdots \rho_m$. We summarize this result in our next theorem.

Theorem 1.3.7 *Let ρ be a permutation of $\{1, \ldots, n\}$. Then ρ can be expressed as a product of disjoint (commuting) cycles.*

It is evident that the expression $\rho = \rho_1 \cdots \rho_m$ that was derived from the orbit decomposition (1.3.3) is unique up to the order of the 'factors' ρ_j. Indeed if $\rho = \mu_1 \cdots \mu_v$, where the μ_i are pairwise disjoint cycles, then the set of points not fixed by μ_i, constitutes an orbit for ρ, so that μ_i must be some ρ_j. In particular, the number m of factors in this product is uniquely determined by ρ, and we shall return to this later. We pause to name this representation of ρ.

Definition 1.3.8 The representation $\rho = \rho_1 \cdots \rho_m$ which is derived from the orbit decomposition (1.3.3), and which is unique up to the order of the factors ρ_j, is called the *standard representation* of ρ as a product of cycles. □

Let us illustrate these ideas with an example. Consider

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

as a permutation of $\{1, \ldots, 9\}$. The orbits of ρ are $\{1, 7, 2\}$, $\{3, 8\}$, $\{4\}$ and $\{5, 6, 9\}$, and the standard representation of ρ as a product of disjoint cycles is $(1\,7\,2)(3\,8)(4)(5\,6\,9)$.

There is an interesting corollary of Theorem 1.3.7. First, if μ is a cycle of length k, then μ^k (that is, μ applied k times) is the identity map. Suppose now that $\rho = \rho_1 \cdots \rho_m$ is the standard representation of ρ, and let d be any positive integer. As the ρ_j commute, we have

$$\rho^d = (\rho_1 \cdots \rho_m)^d = \rho_1^d \cdots \rho_m^d.$$

It follows that if d is the least common multiple of $q_1, \ldots, q_m$, where q_j is the length of the cycle ρ_j, then $\rho^d = I$. For example if $\rho = (1\,3\,4)(2\,9\,5\,6)(7\,8)$, then $\rho^{12} = I$. In fact, it is not difficult to see that the least common multiple d of the q_j is the smallest positive integer t for which $\rho^t = I$. As d divides $n!$, this shows that $\rho^{n!} = I$ for every permutation ρ of $\{1, \ldots, n\}$.

Exercise 1.3

1. Show that
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 9 & 2 & 6 & 8 & 1 & 5 & 3 \end{pmatrix} = (1\,4\,2\,7)(3\,9)(5\,6\,8).$$
2. Show that $(1\,2\,3\,4) = (1\,4)(1\,3)(1\,2)$. Express $(1\,2\,3\,4\,5)$ as a product of 2-cycles. Express $(1\,2\ \ldots\ n)$ as a product of 2-cycles.
3. Express the permutation
$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 10 & 9 & 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix}$$
as a product of cycles, and hence (using Exercise 1.3.2) as a product of 2-cycles. Use this to express ρ^{-1} as a product of 2-cycles.
4. Show that the set $\{I, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ of permutations is a group.
5. Suppose that the permutation ρ of $\{1, \ldots, n\}$ satisfies $\rho^3 = I$. Show that ρ is a product of 3-cycles, and deduce that if n is not divisible by 3 then ρ fixes some k in $\{1, \ldots, n\}$.

1.4 The sign of a permutation

A 2-cycle $(r\ s)$ (which interchanges the distinct integers r and s and leaves all other integers fixed) is called a *transposition*. Notice that $(r\ s) = (s\ r)$, and that $(r\ s)$ is its own inverse. Common experience tells us that any permutation can be achieved by a succession of transpositions, and this suggests the following result.

Theorem 1.4.1 *Every permutation is a product of transpositions.*

Proof As every permutation is a product of cycles, and as for distinct integers a_i we have (by inspection)

$$(a_1\ a_2\ \cdots\ a_p) = (a_1\ a_p) \cdots (a_1\ a_3)(a_1\ a_2), \tag{1.4.1}$$

the result follow immediately. □

In fact (1.4.1) leads to the following quantitative version of Theorem 1.4.1.

Theorem 1.4.2 *Let ρ be a permutation acting on $\{1, \ldots, n\}$, and suppose that ρ partitions $\{1, \ldots, n\}$ into m orbits. Then ρ can be expressed as a composition of $n - m$ transpositions.*

Proof Let $\rho = \rho_1 \cdots \rho_m$ be the standard representation of ρ as a product of disjoint cycles, and let n_j be the length of the cycle ρ_j. Thus $\sum_j n_j = n$. If $n_j \geq 2$ then, from (1.4.1), ρ_j can be written as a product of $n_j - 1$ transpositions. If $n_j = 1$ then ρ_j is the identity, so that no transpositions are needed for this factor. However, in this case $n_j - 1 = 0$. It follows that we can express ρ as a product of $\sum_j (n_j - 1)$ transpositions, and this number is $n - m$. □

We come now to the major result of this section, namely the *number of* transpositions used to express a permutation ρ as a product of transpositions. Although this number is not uniquely determined by ρ, we will show that its *parity* (that is, whether it is even or odd) is determined by ρ. First, however, we prove a preliminary result.

Lemma 1.4.3 *Suppose that the identity permutation I on $\{1, 2, \ldots, n\}$ can be expressed as a product of m transpositions. Then m is even.*

Proof The proof is by induction on n, and we begin with the case $n = 2$. In this case we write $I = \tau_1 \cdots \tau_m$, where each τ_j is the transposition $(1\,2)$. As $(1\,2)^m = (1\,2)$ if m is odd, we see that m must be even, so the conclusion is true when $n = 2$.

We now suppose that the conclusion holds when the permutations act on $\{1, 2, \ldots, n-1\}$, and consider the situation in which $I = \tau_1 \cdots \tau_m$, where each τ_j is a transposition acting on $\{1, \ldots, n\}$. Clearly, $m \neq 1$, thus $m \geq 2$. Suppose, for the moment, that τ_m does not fix n. Then, for a suitable choice of a, b and c, we have one of the following situations:

$$\tau_{m-1}\tau_m = \begin{cases} (n\ b)(n\ a) = (a\ b\ n) = (n\ a)(a\ b); \\ (a\ b)(n\ a) = (a\ n\ b) = (n\ b)(a\ b); \\ (b\ c)(n\ a) = (n\ a)(b\ c); \\ (n\ a)(n\ a) = I = (a\ b)(a\ b). \end{cases}$$

It follows that we can now write I as a product of m transpositions in which the first transposition to be applied fixes n (this was proved under the assumption that $\tau_m(n) \neq n$, and I is already in this form if $\tau_m(n) = n$). In other words, we may assume that $\tau_m(n) = n$. We can now apply the same argument to $\tau_1 \cdots \tau_{m-1}$ (providing that $m - 1 \geq 2$), and the process can be continued to the point where we can write $I = \tau_1 \cdots \tau_m$, where each of $\tau_2, \ldots, \tau_m$ fixes n. But then τ_1 also

fixes n, because

$$\tau_1(n) = \tau_1 \cdots \tau_m(n) = I(n) = n.$$

Thus, we can now write $I = \tau_1 \cdots \tau_m$, where each τ_j is a transposition *acting on* $\{1, \ldots, n-1\}$. The induction hypothesis now implies that m is even and the proof is complete. □

The main result now follows.

Theorem 1.4.4 *Suppose that a permutation ρ can be expressed both as a product of p transpositions, and also as a product of q transpositions. Then p and q are both even, or both odd.*

Proof Suppose that $\tau_1 \cdots \tau_p = \sigma_1 \cdots \sigma_q$, where each τ_i and each σ_j is a transposition. Then $\sigma_q \sigma_{q-1} \cdots \sigma_1 \tau_1 \cdots \tau_p = I$, so that, by Lemma 1.4.3, $p + q$ is even. It follows from this that p and q are both even, or both odd. □

As an example, consider the permutation $\rho = (1\,3\,5)(2\,4\,6\,8)(7)$ acting on $\{1, \ldots, 8\}$. Here, $n = 8$ and $N(\rho) = 3$ so that, by Lemma 1.4.3, ρ can be expressed as a product of five transpositions. Theorem 1.4.4 now implies that if we write ρ as a product of tranpositions *in any way whatsoever*, then there will necessarily be an odd number of transpositions in the product. This discussion suggests the following definition.

Definition 1.4.5 The *sign* $\varepsilon(\rho)$ of a permutation ρ is $(-1)^q$, where ρ can be expressed as a product of q transpositions. We say that ρ is an *even permutation* if $\varepsilon(\rho) = 1$, and an *odd permutation* if $\varepsilon(\rho) = -1$. □

Observe from (1.4.1) that if ρ is a p-cycle then $\varepsilon(\rho) = (-1)^{p+1}$; thus *a cycle of even length is odd*, and *a cycle of odd length is even*. If the permutations α and β can be expressed as products of p and q transpositions, respectively, then the composition $\alpha\beta$ can be expressed as a product of $p + q$ transpositions; thus the next two results are clear.

Theorem 1.4.6 *If α and β are permutations, then $\varepsilon(\alpha\beta) = \varepsilon(\alpha)\varepsilon(\beta)$. In particular, $\varepsilon(\alpha) = \varepsilon(\alpha^{-1})$.*

Theorem 1.4.7 *The product of two even permutations is an even permutation. The inverse of an even permutation is an even permutation. More generally, the set of even permutations in S_n is a group.*

Definition 1.4.8 The *alternating group* A_n is the group of all even permutations in S_n.

It is easy to find the number of elements in the symmetric group S_n and in the alternating group A_n.

Theorem 1.4.9 *The symmetric group S_n has $n!$ elements, and the alternating group A_n has $n!/2$ elements.*

Proof Elementary combinatorial arguments show that S_n has exactly $n!$ elements for, in order to construct a permutation of $\{1, \ldots, n\}$, there are n ways to choose the image of 1, then $n-1$ ways to choose the image of 2 (distinct from the image of 1), and so on. Thus S_n has $n!$ elements.

Now let σ be the transposition $(1\,2)$ and let $f : S_n \to S_n$ be the function defined by $f(\rho) = \sigma\rho$. We note that f is invertible, with $f^{-1} = f$, because, for every ρ, $f(f(\rho)) = f(\sigma\rho) = \sigma\sigma\rho = \rho$. It is clear that f maps even permutations to odd permutations, and odd permutations to even permutations and, as f is invertible, there are the same number of even permutations in S_n as there are odd permutations. Thus there are exactly $n!/2$ even permutations in S_n. □

Theorem 1.4.1 says that every permutation is a product of 2-cycles. Are there any other values of m with the property that every permutation a product of m-cycles? The answer is given in the next theorem.

Theorem 1.4.10 *Let ρ be a permutation of $\{1, \ldots, n\}$, and let m be an integer satisfying $2 \leq m \leq n$. Then ρ is a product of m-cycles if and only if either ρ is an even permutation, or m is an even integer.*

Proof Take any integer m with $2 \leq m \leq n$. Suppose first that ρ is an even permutation. The identity

$$(a_1\,a_2)(a_1\,a_3) = (a_1\,a_2\,a_3\,a_4 \cdots a_m)(a_m \cdots a_4\,a_3\,a_1\,a_2),$$

where the a_i are distinct (and which can be verified by inspection) shows that it suffices to express ρ as a product of terms $\tau_i\tau_j$, where τ_i and τ_j are transpositions with exactly one entry in common. Now as ρ is even it can certainly be be written as a product of terms of the form $\tau_i\tau_j$, where each τ_k is a transposition, and clearly we may assume that $\tau_i \neq \tau_j$. If τ_i and τ_j have no elements in common then we can use the identity

$$(a\,b)(c\,d) = (a\,b)(a\,c)(a\,c)(c\,d),$$

to obtain ρ as a product of the desired terms.

Let us now suppose that ρ is an odd permutation. If ρ is a product of m-cycles, say, $\rho = \rho_1 \cdots \rho_t$, then

$$-1 = \varepsilon(\rho) = \varepsilon(\rho_1) \cdots \varepsilon(\rho_t) = [(-1)^{m-1}]^t,$$

so that m is even. Finally, take any even m, and let $\sigma_0 = (1\,2\,3 \cdots m)$. As σ_0 is odd, we see that $\sigma_0\rho$ is even. It follows that $\sigma_0\rho$, and hence ρ itself, can be written as a product of m-cycles. □

Exercise 1.4

1. Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 2 & 1 & 4 & 3 & 6 \end{pmatrix}$ is odd.
2. Find all six elements of S_3 and determine which are even and which are odd. Find all twelve even permutations of S_4.
3. The *order* of a permutation ρ is the smallest positive integer m such that ρ^m (that is, ρ applied m times) is the identity map.
   (a) What is the order of the permutation $(1\,2\,3\,4)(5\,6\,7\,8\,9)$?
   (b) Which element of S_9 has the highest order, and what is this order?
   (c) Show that every element of order 14 in S_{10} is odd.
4. (i) By considering $(1\,a)(1\,b)(1\,a)$, show that any permutation in S_n can be written as a product of the transpositions $(1, 2), (1\,3), \ldots, (1\,n)$, each of which may be used more than once.
   (ii) Use (i) to show that any permutation in S_n can be written as a product of the transpositions $(1, 2), (2\,3), \ldots, (n-1\,n)$, each of which may be used more than once.
   [This is the basis of bell-ringing, for a bell-ringer can only 'change places' with a neighbouring bell-ringer.]
5. Show that any subgroup of S_n (that is, a subset of S_n that is a group in its own right) which is not contained in A_n contains an equal number of even and odd permutations.

1.5 Permutations of an arbitrary set

This section is devoted to a careful look at functions between arbitrary sets. The reader will have already met functions defined by algebraic rules (for example, $x^2 + 3x + 5$), but we need to understand what one means by a function between sets in the absence of any arithmetic. We can say that a function $f : X \to Y$ is a rule that assigns to each x in X a unique y in Y and this seems clear enough, but what do we actually mean by a rule, and why should it be easier to define a 'rule' than a function? In fact, it is easier to think about a function in terms of its graph, and this is what we shall do next. As an example, the graph $G(f)$ of the function $f(x) = x^2$, where $x \in \mathbb{R}$, is the set

$$G(f) = \{(x, x^2) : x \in \mathbb{R}\} = \{(x, f(x)) \in \mathbb{R}^2 : x \in \mathbb{R}\}$$