

then 4 is fixed, so 3 is mapped to 4 by the composite map. Similarly, 4 is first mapped to 3 then 3 is mapped to 1, completing this cycle in the product:  $(1\ 3\ 4)$ . Finally, 2 is sent to 1, then 1 is sent to 2 so 2 is fixed by this product and so  $(1\ 2\ 3) \circ (1\ 2)(3\ 4) = (1\ 3\ 4)$  is the cycle decomposition of the product.

As additional examples,

$$(12) \circ (13) = (1\ 3\ 2) \quad \text{and} \quad (1\ 3) \circ (1\ 2) = (1\ 2\ 3).$$

In particular this shows that

$S_n$  is a non-abelian group for all  $n \geq 3$ .

Each cycle  $(a_1\ a_2\ \dots\ a_m)$  in a cycle decomposition can be viewed as the permutation which cyclically permutes  $a_1, a_2, \dots, a_m$  and fixes all other integers. Since disjoint cycles permute numbers which lie in disjoint sets it follows that

*disjoint cycles commute.*

Thus rearranging the cycles in any product of disjoint cycles (in particular, in a cycle decomposition) does not change the permutation.

Also, since a given cycle,  $(a_1\ a_2\ \dots\ a_m)$ , permutes  $\{a_1, a_2, \dots, a_m\}$  cyclically, the numbers in the cycle itself can be cyclically permuted without altering the permutation, i.e.,

$$\begin{aligned} (a_1\ a_2\ \dots\ a_m) &= (a_2\ a_3\ \dots\ a_m\ a_1) = (a_3\ a_4\ \dots\ a_m\ a_1\ a_2) = \dots \\ &= (a_m\ a_1\ a_2\ \dots\ a_{m-1}). \end{aligned}$$

Thus, for instance,  $(1\ 2) = (2\ 1)$  and  $(1\ 2\ 3\ 4) = (3\ 4\ 1\ 2)$ . By convention, the smallest number appearing in the cycle is usually written first.

One must exercise some care working with cycles since a permutation may be written in many ways as an arbitrary product of cycles. For instance, in  $S_3$ ,  $(1\ 2\ 3) = (1\ 2)(2\ 3) = (1\ 3)(1\ 3\ 2)(1\ 3)$  etc. But, (as we shall prove) the cycle decomposition of each permutation is the *unique* way of expressing a permutation as a product of disjoint cycles (up to rearranging its cycles and cyclically permuting the numbers within each cycle). Reducing an arbitrary product of cycles to a product of disjoint cycles allows us to determine at a glance whether or not two permutations are the same. Another advantage to this notation is that it is an exercise (outlined below) to prove that *the order of a permutation is the l.c.m. of the lengths of the cycles in its cycle decomposition.*

## EXERCISES

1. Let  $\sigma$  be the permutation

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$$

and let  $\tau$  be the permutation

$$1 \mapsto 5 \quad 2 \mapsto 3 \quad 3 \mapsto 2 \quad 4 \mapsto 4 \quad 5 \mapsto 1.$$

Find the cycle decompositions of each of the following permutations:  $\sigma$ ,  $\tau$ ,  $\sigma^2$ ,  $\sigma\tau$ ,  $\tau\sigma$ , and  $\tau^2\sigma$ .

2. Let  $\sigma$  be the permutation

$1 \mapsto 13$	$2 \mapsto 2$	$3 \mapsto 15$	$4 \mapsto 14$	$5 \mapsto 10$
$6 \mapsto 6$	$7 \mapsto 12$	$8 \mapsto 3$	$9 \mapsto 4$	$10 \mapsto 1$
$11 \mapsto 7$	$12 \mapsto 9$	$13 \mapsto 5$	$14 \mapsto 11$	$15 \mapsto 8$

and let  $\tau$  be the permutation

$1 \mapsto 14$	$2 \mapsto 9$	$3 \mapsto 10$	$4 \mapsto 2$	$5 \mapsto 12$
$6 \mapsto 6$	$7 \mapsto 5$	$8 \mapsto 11$	$9 \mapsto 15$	$10 \mapsto 3$
$11 \mapsto 8$	$12 \mapsto 7$	$13 \mapsto 4$	$14 \mapsto 1$	$15 \mapsto 13$

Find the cycle decompositions of the following permutations:  $\sigma$ ,  $\tau$ ,  $\sigma^2$ ,  $\sigma\tau$ ,  $\tau\sigma$ , and  $\tau^2\sigma$ .

- For each of the permutations whose cycle decompositions were computed in the preceding two exercises compute its order.
- Compute the order of each of the elements in the following groups: (a)  $S_3$  (b)  $S_4$ .
- Find the order of  $(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$ .
- Write out the cycle decomposition of each element of order 4 in  $S_4$ .
- Write out the cycle decomposition of each element of order 2 in  $S_4$ .
- Prove that if  $\Omega = \{1, 2, 3, \dots\}$  then  $S_\Omega$  is an infinite group (do not say  $\infty! = \infty$ ).
- (a) Let  $\sigma$  be the 12-cycle  $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$ . For which positive integers  $i$  is  $\sigma^i$  also a 12-cycle?  
(b) Let  $\tau$  be the 8-cycle  $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ . For which positive integers  $i$  is  $\tau^i$  also an 8-cycle?  
(c) Let  $\omega$  be the 14-cycle  $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14)$ . For which positive integers  $i$  is  $\omega^i$  also a 14-cycle?
- Prove that if  $\sigma$  is the  $m$ -cycle  $(a_1\ a_2\ \dots\ a_m)$ , then for all  $t \in \{1, 2, \dots, m\}$ ,  $\sigma^i(a_k) = a_{k+i}$ , where  $k+i$  is replaced by its least residue mod  $m$  when  $k+i > m$ . Deduce that  $|\sigma| = m$ .
- Let  $\sigma$  be the  $m$ -cycle  $(1\ 2\ \dots\ m)$ . Show that  $\sigma^i$  is also an  $m$ -cycle if and only if  $i$  is relatively prime to  $m$ .
- (a) If  $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$  determine whether there is a  $n$ -cycle  $\sigma$  ( $n \geq 10$ ) with  $\tau = \sigma^k$  for some integer  $k$ .  
(b) If  $\tau = (1\ 2)(3\ 4\ 5)$  determine whether there is an  $n$ -cycle  $\sigma$  ( $n \geq 5$ ) with  $\tau = \sigma^k$  for some integer  $k$ .
- Show that an element has order 2 in  $S_n$  if and only if its cycle decomposition is a product of commuting 2-cycles.
- Let  $p$  be a prime. Show that an element has order  $p$  in  $S_n$  if and only if its cycle decomposition is a product of commuting  $p$ -cycles. Show by an explicit example that this need not be the case if  $p$  is not prime.
- Prove that the order of an element in  $S_n$  equals the least common multiple of the lengths of the cycles in its cycle decomposition. [Use Exercise 10 and Exercise 24 of Section 1.]
- Show that if  $n \geq m$  then the number of  $m$ -cycles in  $S_n$  is given by

$$\frac{n(n-1)(n-2)\dots(n-m+1)}{m}.$$

[Count the number of ways of forming an  $m$ -cycle and divide by the number of representations of a particular  $m$ -cycle.]

17. Show that if  $n \geq 4$  then the number of permutations in  $S_n$  which are the product of two disjoint 2-cycles is  $n(n-1)(n-2)(n-3)/8$ .
18. Find all numbers  $n$  such that  $S_5$  contains an element of order  $n$ . [Use Exercise 15.]
19. Find all numbers  $n$  such that  $S_7$  contains an element of order  $n$ . [Use Exercise 15.]
20. Find a set of generators and relations for  $S_3$ .

## 1.4 MATRIX GROUPS

In this section we introduce the notion of matrix groups where the coefficients come from fields. This example of a family of groups will be used for illustrative purposes in Part I and will be studied in more detail in the chapters on vector spaces.

A *field* is the “smallest” mathematical structure in which we can perform all the arithmetic operations  $+$ ,  $-$ ,  $\times$ , and  $\div$  (division by nonzero elements), so in particular every nonzero element must have a multiplicative inverse. We shall study fields more thoroughly later and in this part of the text the only fields  $F$  we shall encounter will be  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{Z}/p\mathbb{Z}$ , where  $p$  is a prime. The example  $\mathbb{Z}/p\mathbb{Z}$  is a finite field, which, to emphasize that it is a field, we shall denote by  $\mathbb{F}_p$ . For the sake of completeness we include here the precise definition of a field.

### Definition.

- (1) A *field* is a set  $F$  together with two binary operations  $+$  and  $\cdot$  on  $F$  such that  $(F, +)$  is an abelian group (call its identity 0) and  $(F - \{0\}, \cdot)$  is also an abelian group, and the following *distributive* law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad \text{for all } a, b, c \in F.$$

- (2) For any field  $F$  let  $F^\times = F - \{0\}$ .

All the vector space theory, the theory of matrices and linear transformations and the theory of determinants when the scalars come from  $\mathbb{R}$  is true, *mutatis mutandis*, when the scalars come from an arbitrary field  $F$ . When we use this theory in Part I we shall state explicitly what facts on fields we are assuming.

For each  $n \in \mathbb{Z}^+$  let  $GL_n(F)$  be the set of all  $n \times n$  matrices whose entries come from  $F$  and whose determinant is nonzero, i.e.,

$$GL_n(F) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\},$$

where the determinant of any matrix  $A$  with entries from  $F$  can be computed by the same formulas used when  $F = \mathbb{R}$ . For arbitrary  $n \times n$  matrices  $A$  and  $B$  let  $AB$  be the product of these matrices as computed by the same rules as when  $F = \mathbb{R}$ . This product is associative. Also, since  $\det(AB) = \det(A) \cdot \det(B)$ , it follows that if  $\det(A) \neq 0$  and  $\det(B) \neq 0$ , then  $\det(AB) \neq 0$ , so  $GL_n(F)$  is closed under matrix multiplication. Furthermore,  $\det(A) \neq 0$  if and only if  $A$  has a matrix inverse (and this inverse can be computed by the same adjoint formula used when  $F = \mathbb{R}$ ), so each  $A \in GL_n(F)$  has an inverse,  $A^{-1}$ , in  $GL_n(F)$ :

$$AA^{-1} = A^{-1}A = I,$$

where  $I$  is the  $n \times n$  identity matrix. Thus  $GL_n(F)$  is a group under matrix multiplication, called the *general linear group of degree  $n$* .

The following results will be proved in Part III but are recorded now for convenience:

- (1) if  $F$  is a field and  $|F| < \infty$ , then  $|F| = p^m$  for some prime  $p$  and integer  $m$
- (2) if  $|F| = q < \infty$ , then  $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$ .

## EXERCISES

Let  $F$  be a field and let  $n \in \mathbb{Z}^+$ .

1. Prove that  $|GL_2(\mathbb{F}_2)| = 6$ .
2. Write out all the elements of  $GL_2(\mathbb{F}_2)$  and compute the order of each element.
3. Show that  $GL_2(\mathbb{F}_2)$  is non-abelian.
4. Show that if  $n$  is not prime then  $\mathbb{Z}/n\mathbb{Z}$  is not a field.
5. Show that  $GL_n(F)$  is a finite group if and only if  $F$  has a finite number of elements.
6. If  $|F| = q$  is finite prove that  $|GL_n(F)| < q^{n^2}$ .
7. Let  $p$  be a prime. Prove that the order of  $GL_2(\mathbb{F}_p)$  is  $p^4 - p^3 - p^2 + p$  (do not just quote the order formula in this section). [Subtract the number of  $2 \times 2$  matrices which are *not* invertible from the total number of  $2 \times 2$  matrices over  $\mathbb{F}_p$ . You may use the fact that a  $2 \times 2$  matrix is not invertible if and only if one row is a multiple of the other.]
8. Show that  $GL_n(F)$  is non-abelian for any  $n \geq 2$  and any  $F$ .
9. Prove that the binary operation of matrix multiplication of  $2 \times 2$  matrices with real number entries is associative.
10. Let  $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$ .
  - (a) Compute the product of  $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$  and  $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$  to show that  $G$  is closed under matrix multiplication.
  - (b) Find the matrix inverse of  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$  and deduce that  $G$  is closed under inverses.
  - (c) Deduce that  $G$  is a subgroup of  $GL_2(\mathbb{R})$  (cf. Exercise 26, Section 1).
  - (d) Prove that the set of elements of  $G$  whose two diagonal entries are equal (i.e.,  $a = c$ ) is also a subgroup of  $GL_2(\mathbb{R})$ .

The next exercise introduces the *Heisenberg group* over the field  $F$  and develops some of its basic properties. When  $F = \mathbb{R}$  this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interpretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally — for example, with entries in  $\mathbb{Z}$ .

11. Let  $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$  — called the *Heisenberg group over  $F$* . Let  $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$  and  $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$  be elements of  $H(F)$ .
  - (a) Compute the matrix product  $XY$  and deduce that  $H(F)$  is closed under matrix multiplication. Exhibit explicit matrices such that  $XY \neq YX$  (so that  $H(F)$  is always non-abelian).