1

Groups and permutations

1.1 Introduction

This text is about the interaction between algebra and geometry, and central to this interaction is the idea of a group. Groups are studied as abstract systems in algebra; they help us to describe the arithmetic structure of the real and complex numbers, and modular arithmetic, and they provide a framework for a discussion of permutations of an arbitrary set. Groups also arise naturally in geometry; for example, as the set of translations of the plane, the rotations of the plane about the origin, the symmetries of a cube, and the set of all functions of the plane into itself that preserve distance. We shall see that geometry provides many other interesting examples of groups and, in return, group theory provides a language and a number of fundamental ideas which can be used to give a precise description of geometry. In 1872 Felix Klein proposed his *Erlangen Programme* in which, roughly speaking, he suggested that we should study different geometries by studying the groups of transformations acting on the geometry. It is this spirit that this text has tried to capture.

We shall assume familiarity with the most basic facts about elementary set theory. We recall that if X is any set, then $x \in X$ means that x is an *element*, or *member*, of X, and $x \notin X$ means that x is not an element of X. The *union* $X \cup Y$ of two sets X and Y is the set of objects that are in at least one of them; the *intersection* $X \cap Y$ is the set of objects that are in both. The *difference set* $X \backslash Y$ is the set of objects that are in X but not in Y. The *empty set* $\emptyset$ is the set with no elements in it; for example, $X \backslash X = \emptyset$ for every set X. We say that X is *non-empty* when $X \neq \emptyset$.

In this chapter we shall define what we mean by a group, and then show that every non-empty set X has associated with it a group, which is known as the group of permutations of X. This basic fact underpins almost everything in this book. We shall also carry out a detailed study of the group of permutations

of the finite set $\{1, 2, \ldots, n\}$ of integers. In Chapter 2 we review the algebraic properties of the real numbers in terms of groups, but in order to give concrete examples of groups now, we shall assume (in the examples) familiarity with the real numbers. Throughout the book we use $\mathbb{Z}$ for the set of integers, $\mathbb{Q}$ for the set of rational numbers, and $\mathbb{R}$ for the set of real numbers.

1.2 Groups

There are four properties that are shared by many mathematical systems and that have proved their usefulness over time, and any system that possesses these is known as a *group*. It is difficult to say when groups first appeared in mathematics for the ideas were used long before they were synthesized into an abstract definition of a group. Euler (1761) and Gauss (1801) studied modular arithmetic (see Section 2.4), and Lagrange (1770) and Cauchy (1815) studied groups of permutations (see Section 1.3). Important moves towards a more formal, abstract theory were taken by Cauchy (1845), von Dyck (1882) and Burnside (1897), thus group theory, as we know it today, is a relative newcomer to the history of mathematics.

First, we introduce the notion of a binary operation on a set X. A *binary operation* $*$ on X is a rule which is used to combine any two elements, say x and y, of X to obtain a third object, which we denote by $x*y$. In many cases $x*y$ will also be in X, and when this is so we say that X is *closed* with respect to $*$. We can now say what we mean by a group.

Definition 1.2.1 A *group* is a set G, together with a binary operation $*$ on G which has the following properties:

(1) for all g and h in G, $g*h \in G$;
(2) for all f, g and h in G, $f*(g*h) = (f*g)*h$;
(3) there a unique e in G such that for all g in G, $g*e = g = e*g$;
(4) if $g \in G$ there is some h in G such that $g*h = e = h*g$. □

A set X may support many different binary operations which make it a group so, for clarification, we often use the phrase '*X is a group with respect to $*$*'. Property (1) is called the *closure axiom* for it says that G is closed with respect to $*$. Property (2) is the *associative law*, and this says that $f * g * h$ is uniquely defined regardless of which of the two operations $*$ we choose to do first. The point here is that as $*$ only combines *two* objects at a time, we have to apply $*$ twice (in some order) to obtain $f*g*h$. There are exactly two ways to do

this, and (2) says that these two ways must yield the same result. Obviously, this idea extends to more elements, and reader should now use (2) to verify that the element $f*g*h*i$ is defined independently of the order in which the three applications of $*$ are carried out. It is important to understand that the associative law is not self-evident; indeed, if $a*b = a/b$ for for positive numbers a and b then, in general, $(a*b)*c \neq a*(b*c)$.

The element e in (3) is the *identity element* of G, and the reader should note that (3) requires that *both* $e*g$ and $g*e$ are g. In the example just considered (where $a*b = a/b$) we have $a*1 = a$ but $1*a \neq a$ (unless $a = 1$). We also note that in conjunction with (1) and (2), we could replace (3) by the weaker statement that there exists some e in G such that $g*e = g = e*g$ for every g in G. Indeed, suppose that G contains elements e and e' such that, for all g in G, $g*e = g = e*g$ and $g*e' = g = e'*g$. Then $e' = e*e' = e$ so that $e' = e$ (so that such an element is necessarily unique). It follows that when we need to prove that, say, G is a group we need only prove the existence of some element e in G such that $e*g = g = g*e$ for every g (and it is not necessary to prove the uniqueness of e). However, we cannot replace (3) by this weaker version of (3) in the definition of a group without making (4) ambiguous.

The element h in (4) is the *inverse of* g, and henceforth will be written as g^{-1}. However, before we can legitimately speak of *the* inverse of g, and use the notation g^{-1}, we need to show that each g has only one inverse.

Lemma 1.2.2 *Let G be any group. Then, given g in G, there is only one element h that satisfies* (4). *In particular,* $(g^{-1})^{-1} = g$.

Proof Take any g and suppose that h and h' satisfy $h*g = e = g*h$ and $h'*g = e = g*h'$. Then

$$h = h*e = h*(g*h') = (h*g)*h' = e*h' = h'$$

as required. As $g*g^{-1} = e = g^{-1}*g$, it is clear that $(g^{-1})^{-1} = g$. □

The next three results show that one can manipulate expressions, and solve simple equations, in groups much as one does for real numbers.

Lemma 1.2.3 *Suppose that a, b and x are in a group G. If $a*x = b*x$ then $a = b$. Similarly, if $x*a = x*b$ then $a = b$.*

Proof If $a*x = b*x$ then $(a*x)*x^{-1} = (b*x)*x^{-1}$. Now $(a*x)*x^{-1} = a*(x*x^{-1}) = a*e = a$, and similarly for b instead of a; thus $a = b$. The second statement follows in a similar way. For obvious reasons, this result is known as the *cancellation law*. □

Lemma 1.2.4 *Suppose that a and b are in a group G. Then the equation $a*x = b$ has a unique solution in G, namely $x = a^{-1}*b$. Similarly, $x*a = b$ has a unique solution, namely $b*a^{-1}$.*

Proof As $a*(a^{-1}*b) = (a*a^{-1})*b = e*b = b$, we see that $a^{-1}*b$ is a solution of $a*x = b$. Now let y_1 and y_2 be any solutions. Then $a*y_1 = b = a*y_2$ so that, by Lemma 1.2.3, $y_1 = y_2$. The second statement follows in a similar way. □

Lemma 1.2.5 *In any group G, e is the unique solution of $x*x = x$.*

Proof As $y*e = y$ for every y, we see that $e*e = e$. Thus e is one solution of $x*x = x$. However, if $x*x = x$ then $x*x = x*e$ so that from Lemma 1.2.3, $x = e$. □

The reader should note that the definition of a group does *not* include the assumption that $f*g = g*f$; indeed, there are many interesting groups in which equality does not hold. However, this condition is so important that it carries its own terminology.

Definition 1.2.6 Let G be a group with respect to $*$. We say that f and g in G *commute* if $f*g = g*f$. If $f*g = g*f$ for every f and g in G, we say that G is an *abelian*, or a *commutative*, group. We often abbreviate this to 'G is abelian'. □

Several straightforward examples of groups are given in the Exercises. We end this section with an example of a non-commutative group.

Example 1.2.7 Let G be the set of functions of the form $f(x) = ax + b$, where a and b are real numbers and $a \neq 0$. It is easy to see that G is a group with respect to the operation $*$ defined by making $f*g$ the function $f(g(x))$. First, if $g(x) = ax + b$ and $h(x) = cx + d$, then $g*h$ is in G because $(g*h)(x) = g(h(x)) = acx + (ad + b)$. It is also easy (though tedious) to check that for any f, g and h in G, $f*(g*h) = (f*g)*h$. Next, the function $e(x) = 1x + 0$ is in G and satisfies $e*f = f = f*e$ for every f in G. Finally, if $g(x) = ax + b$ then $g*g^{-1} = e = g^{-1}*g$, where $g^{-1}(x) = x/a - b/a$. We have shown that G is a group, but it is *not* abelian as $f*g \neq g*f$ when $f(x) = x + 1$ and $g(x) = -x + 1$. In the same way we see that the set of functions of the form $f(x) = ax + n$, where $a = \pm 1$ and n is an integer is also a non-abelian group. □

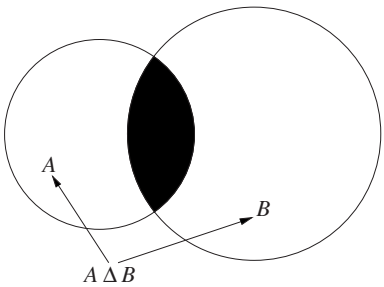

Figure 1.2.1

Exercise 1.2

1. Show that the set $\mathbb{Z}$ is a group with respect to addition. Show also that the set of positive real numbers is a group with respect to multiplication.
2. Let $\mathbb{Q}$ be the set of rational numbers (that is, numbers of the form m/n where m and n are integers and $n \neq 0$), and let $\mathbb{Q}^+$ and $\mathbb{Q}^*$ be the set of positive, and non-zero, rational numbers, respectively. Show that $\mathbb{Q}$, but not $\mathbb{Q}^+$, is a group with respect to addition. Show that $\mathbb{Q}^+$ and $\mathbb{Q}^*$ are groups with respect to with respect to multiplication, but that $\mathbb{Q}$ is not. Is the set of rational numbers of the form p/q, where p and q are positive odd integers, a group with respect to multiplication?
3. Show that $\mathbb{Z}$, with the operation $*$ defined by $m*n = m + n + 1$, is a group. What is the identity element in this group? Show that the inverse of n is $-(n + 2)$.
4. Show that $\mathbb{Z}$, with the operation $m*n = m + (-1)^m n$, is a group. Show that in this group the inverse n^{-1} of n is $(-1)^{n+1}n$. For which n is $n^{-1} = n$?
5. Let $G = \{x \in \mathbb{R} : x \neq -1\}$, where $\mathbb{R}$ is the set of real numbers, and let $x*y = x + y + xy$, where xy denotes the usual product of two real numbers. Show that G with the operation $*$ is a group. What is the inverse 2^{-1} of 2 in this group? Find $(2^{-1})*6*(5^{-1})$, and hence solve the equation $2*x*5 = 6$.
6. For any two sets A and B the *symmetric difference* $A\Delta B$ of A and B is the set of elements in *exactly one* of A and B; thus

$$A\Delta B = \{x \in A \cup B : x \notin A \cap B\} = (A \cup B)\backslash(A \cap B)$$

(see Figure 1.2.1). Let Ω be a non-empty set and let G be the set of subsets of Ω (note that G includes both the empty set $\emptyset$ and Ω). Show that G with the operation Δ is a group with $\emptyset$ as the identity element of G. What is A^{-1}? Now let $\Omega = \{1, 2, \ldots, 7\}$, $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$ and

$C = \{5, 6, 7\}$. 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 $\{1, \dots, n\}$. □

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 $\{1, \dots, 9\}$, 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 $\{1, \dots, n\}$ 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 $\{1, \dots, n\}$, 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 $\{1, \dots, n\}$. 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* $(n_1 \dots n_q)$ 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 $1 \le j < q$, and n_q to n_1, and it fixes all other integers in $\{1, \dots, n\}$. 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 $\{1, \dots, n\}$, 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

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

the *orbit* of k under ρ. Now every point m in $\{1, \dots, n\}$ 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

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

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 $\{1, \dots, n\}$.

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 $\{1, \dots, n\}$ 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 $\{1, \dots, n\}$. 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 $\{1, \dots, 9\}$. 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

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