Chapter 6
Permutations

A *permutation* is a bijection from a set S to itself. We shall take S to be finite in this Chapter. We shall also introduce a new notation for functions. Instead of using the notation $f(x)$ (where x is a member of some set S and $f : S \to T$ a function) we shall use the more compact notation xf. In this notation f goes on the right, which will facilitate some of our calculations with permutations. If $g : T \to U$ then xfg means : take x, apply f and then apply g, in other words xfg is $g(f(x))$ in the notation we used in Chapter 2.

We usually label elements of our finite set S by $1, 2, \ldots, n$. We adopt the "two line" notation for permutations.

Examples

1. Let $S = \{1, 2, 3, 4\}$ and let $\alpha : S \to S$ be the bijection given by $\alpha(1) = 4$, $\alpha(2) = 3$, $\alpha(3) = 1$ and $\alpha(4) = 2$. In our new notation this is $1\alpha = 4$, $2\alpha = 3$, $3\alpha = 1$ and $4\alpha = 2$. We represent α by

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

2. We take $S = \{1, 2, 3, 4, 5\}$ and let $\alpha : S \to S$ be the bijection given by $1\alpha = 3$, $2\alpha = 1$, $3\alpha = 4$, $4\alpha = 2$, $5\alpha = 5$. We represent α by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}.$$

Notation

Given a permutation α of the set $\{1, 2, \ldots, n\}$ we represent α by

$$\begin{pmatrix} 1 & 2 & \cdot & \cdot & \cdot & n \\ a_1 & a_2 & \cdot & \cdot & \cdot & a_n \end{pmatrix}$$

where $1\alpha = a_1, 2\alpha = a_2, \ldots, n\alpha = a_n$. This is called the *two line notation.*

Lemma 6.1 *There are $n!$ different permutations of $\{1, 2, \ldots, n\}$.*

Composition of Permutations

The two line notation makes it easy to calculate $\alpha\beta$, given permutations α, β.

Example For $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ we have

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

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

Notation

(i) We write α^k for $\alpha\alpha\ldots\alpha$ (k times).

(ii) We write ι (iota) for the identity permutation, that is to say the map given by $x\iota = x$, for all $x \in S$.

In two line notation ι is $\begin{pmatrix} 1 & 2 & \cdot & \cdot & \cdot & n \\ 1 & 2 & \cdot & \cdot & \cdot & n \end{pmatrix}$. Note that $\alpha\iota = \iota\alpha = \alpha$, for every permutation α.

A permutation has an inverse (since it is a bijection). We write α^{-1} for the inverse of α. We define α^{-r} to be $\alpha^{-1}\alpha^{-1}\ldots\alpha^{-1}$, the inverse of α^r. We define α^0 to be ι.

Lemma 6.2 *Let α be a permutation. Then there exists a positive integer k such that $\alpha^k = \iota$.*

Definition The *order* of a permutation α is the smallest positive integer m such that $\alpha^m = \iota$.

Lemma 6.3 *Let m be the order of α. Then $\alpha^k = \iota$ if and only if m divides k.*

Notation Suppose $a_1, a_2, \ldots, a_r$ are distinct elements of $\{1, 2, \ldots, n\}$. Write $(a_1 a_2 \ldots a_r)$ for the permutation taking a_1 to $_2$, taking a_2 to a_3,..., taking a_{r-1} to a_r, taking a_r to a_1 and leaving all other elements fixed. We call $(a_1 a_2 \ldots a_r)$ a *cycle* and call r the *length* of the cycle.

Example For $n = 5$, the cycle (314) is the permutation taking 3 to 1, taking 1 to 4 and taking 4 to 3. In two line notation this is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$.

Sometimes we put in the cycles of length 1, but usually we miss them out, so we can write

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} = (314)$$

or

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} = (314)(2)(5).$$

Note that in fact a cycle (a) of length one is the identity (it takes a to a and leaves all other elements fixed too).

Lemma 6.4 *Every cycle of length r has order r.*

We shall prove that every permutation is a product of disjoint cycles (cycles no two of which contain a common element) but first we look at some examples.

Examples
1. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 5 & 1 & 7 & 2 & 3 \end{pmatrix}$. So α takes 1 to 6, takes 6 to 2, takes 2 to 4 and takes 4 to 1, giving the cycle (1624). Also α takes 3 to 5, takes 5 to 7 and takes 7 to 3 giving (357). We get $\alpha = (1624)(357)$.

2. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$. Then $\alpha = (17)(26)(35)(4)$.

Definition Permutations α and β *commute* if $\alpha\beta = \beta\alpha$.

Example Let $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Then $\alpha\beta = \iota = \beta\alpha$ so α and β commute.

Definition Cycles $(a_1 a_2 \dots a_r)$ and $(b_1 b_2 \dots b_s)$ are *disjoint* if no a_i is equal to a b_j.

Example (124) and (356) are disjoint cycles, but (132) and (234) are not.

Lemma 6.5 *Disjoint cycles commute, i.e. if $\alpha = (a_1 \dots a_r)$ and $\beta = (b_1 \dots b_s)$ are disjoint cycles then $\alpha\beta = \beta\alpha$.*

Definition Let α be a permutation of $S = \{1, 2, \dots, n\}$ and let $x \in S$. The *orbit* of x under α is the set of elements $\{x, x\alpha, x\alpha^2, \dots\}$.

Example For $\alpha = (1624)(357)$ the orbit of 1 is $\{1, 6, 2, 4\}$ and the orbit of 3 is $\{3, 5, 7\}$.

Notation Let α be a permutation of $S = \{1, 2, \dots, n\}$. Define a relation $\sim$ on S by $x \sim y$ if $y = x\alpha^k$, for some integer k.

Lemma 6.6
(i) $\sim$ is an equivalence relation.
(ii) The orbit of $x \in \{1, 2, \dots, n\}$ is the equivalence class containing x.

Let α be a permutation and E an orbit. Pick $a \in E$. Note that if α has order m then $\alpha^m = \iota$ so $a\alpha^m = a\iota = a$. Let r be the smallest positive integer such that $a\alpha^r = a$ and put $a_1 = a, a_2 = a\alpha, \dots, a_r = a\alpha^{r-1}$.

We claim that $a_1, \ldots, a_r$ are all different. If not, we have $a_i = a_j$ for some $1 \leq i < j \leq r$, and so $a\alpha^{i-1} = a\alpha^{j-1}$ giving $a\alpha^i = a\alpha^j$ and hence $a = a\alpha^{j-i}$. But $j - i < r$, and r is the smallest positive integer such that $a\alpha^r = a$, so this is impossible.

Hence the $a_1, \ldots, a_r$ are distinct and $(a_1 \ldots a_r) = c$, say, is a cycle. Since $\{a, a\alpha, \ldots\} = \{a_1, \ldots, a_r\}$ we see that $\{a_1, \ldots, a_r\} = E$, the orbit of a. [Remember that in writing down a cycle the order is important, e.g. $(123) \neq (132)$, but in writing down an orbit it is not: $\{1, 2, 3\} = \{1, 3, 2\}$.]

Now if $x \in E$ then $x = a_i$ for some $1 \leq i \leq r$ so that $x\alpha = a_i\alpha = a\alpha^{i-1}\alpha = a\alpha^i$, which is a_{i+1} if $i \neq r$ and if $i = r$ we get $x\alpha = a\alpha^r = a = a_1$. So we have

$$a_i\alpha = \begin{cases} a_{i+1}, & \text{if } i < r; \\ a_1, & \text{if } i = r \end{cases}$$

$$= a_i c.$$

To summarise, we have shown the following.

Lemma 6.7 *Let E be an orbit of α and let c be the associated cycle, constructed as above. Then we have*

$$xc = \begin{cases} x\alpha, & \text{if } x \in E; \\ x, & \text{if } x \notin E. \end{cases}$$

Example For $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ we have an orbit $E = \{1, 2, 4\}$, the corresponding cycle $c = (124)$, and

$$xc = \begin{cases} x\alpha, & \text{if } x \in \{1, 2, 4\}; \\ x, & \text{if } x = 3. \end{cases}$$

Proposition 6.8 *Every permutation can be written as a product of disjoint cycles.*

Example For $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ we have $\alpha = (13)(2)(45)$.

Proposition 6.9 *The cycle decomposition is unique, i.e. if*

$$\alpha = c_1 c_2 \ldots c_s = d_1 d_2 \ldots d_t$$

where $c_1, \ldots, c_s$ are disjoint cycles and where $d_1, \ldots, d_t$ are disjoint cycles then $s = t$ and, after reordering the d_j's if necessary, we have $c_1 = d_1, \ldots, c_s = d_s$.

Properties of cycles and cycle decompositions

1) Let $d_1, \ldots, d_s$ be positive integers. The least common multiple m, say, is the smallest positive integer divisible by $d_1, \ldots, d_s$.
Suppose that α has cycles decomposition $\alpha = c_1 \ldots c_s$, and d_i is the length of the cycle c_i. *Then the order of α is the least common multiple of $d_1, \ldots, d_s$.*

Examples (124)(3657) has order the lcm (least common multiple) of 3 and 4, namely 12.
(12)(5768)(34) has order the lcm of $2, 4, 2$, namely 4.

2) Call permutations α and β *conjugate* if there is some permutation γ such that $\beta = \gamma\alpha\gamma^{-1}$. Suppose we write α as a product of disjoint cycles $c_1, c_2, \ldots, c_s$ of lengths $r_1 \geq r_2 \geq \cdots \geq r_s$. The sequence $(r_1, r_2, \ldots, r_s)$ is called the *cycle type* of α. *Permutations α and γ are conjugate if and only if they have the same cycle type.*

Examples
1. (12)(3564) and (34)(1526) are conjugate (they both have cycle type $(4, 2)$).
2. (123)(456) and (12)(34)(56) are not conjugate. (The first has cycle type $(3, 3)$ and the second has cycle type $(2, 2, 2)$.)

Parity

Permutations come in two types : even and odd.

Definition A *transposition* is a permutation which interchanges two elements and leaves all others fixed. So a transposition is a cycle of length 2, i.e. (ab), for some $a, b \in \{1, 2, \ldots, n\}$ with $a \neq b$.

Proposition 6.10 *Any permutation is a product of transpositions.*

Example $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (123)(45) = (13)(23)(45)$.

We would like to say that a permutation is even if it can be written as a product of an even number of transpositions and odd if it can be written as an odd number of transpositions. But how do we know that some permutation can't be written in one way as a product of an even number of transpositions and in another way as a product of an odd number? One way to see this is as follows.

Definition An $n \times n$ matrix A is called a *permutation matrix* if all its entries are 0's and 1's and it has just one non-zero entry in each row and column.

If α is a permutation of the set $\{1, 2, \ldots, n\}$ we can associate to it the permutation matrix $A(\alpha)$ which has $a_{ij} = 1$ whenever $i\alpha = j$ and $a_{ij} = 0$ for all other pairs $\{i, j\}$.

Proposition 6.11 $A(\alpha\beta) = A(\alpha)A(\beta)$

Let $|A|$ denote the *determinant* of the matrix A. (This is always $+1$ or -1 for a permutation matrix.)

Corollary 6.12 $|A(\alpha\beta)| = |A(\alpha)||A(\beta)|$

Definition A permutation α is said to be *even* if and only if $|A(\alpha)| = +1$ and *odd* if and only if $|A(\alpha)| = -1$.

Proposition 6.13 *A permutation α is even if and only if it can be written as a product of an even number of transpositions, and it is odd if and only if it can be written as a product of an odd number of transpositions.*

Groups

The set S_n of all permutations of $\{1, 2, \ldots, n\}$ is an example of an algebraic structure called a *group*.

A group G is a set equipped with a multiplication such that:
1) it is associative: $(ab)c = (ab)c$ for all $a, b, c \in G$;
2) there is an identity element $e \in G$ such that $ae = a = ea$ for all $a \in G$;
3) every $a \in G$ has an inverse a^{-1} such that $aa^{-1} = a^{-1}a = e$.

S_n is a group, with ι as its identity element. Another example of a group is $\{+1, -1\}$, with the usual multiplication.

Corollary 6.12 says that the map ϕ from S_n to $\{+1, -1\}$ defined by $\alpha \mapsto |A(\alpha)|$ has the property that $\phi(\alpha\beta) = \phi(\alpha).\phi(\beta)$. Maps with this property are called *group homomorphisms*. They will be studied in the course MAS201 Algebraic Structures I.