5. Show that any finitely generated subgroup of the additive group of rationals $(\mathbb{Q}, +, 0)$ is cyclic. Use this to prove that this group is not isomorphic to the direct product of two copies of it.
6. Let a, b be as in Lemma 1. Show that $\langle a\rangle \cap \langle b\rangle = 1$ and $\langle a, b\rangle = \langle ab\rangle$.
7. Show that if $o(a) = n = rs$, where $(r, s) = 1$, then $\langle a\rangle \cong \langle b\rangle \times \langle c\rangle$, where $o(b) = r$ and $o(c) = s$. Hence prove that any finite cyclic group is isomorphic to a direct product of cyclic groups of prime power orders.

1.6 CYCLE DECOMPOSITION OF PERMUTATIONS

A permutation γ of $\{1, 2, \ldots, n\}$ which permutes a sequence of elements $i_1, i_2, \ldots, i_r$, $r > 1$, cyclically in the sense that

$$\gamma(i_1) = i_2, \quad \gamma(i_2) = i_3, \ldots, \gamma(i_{r-1}) = i_r, \quad \gamma(i_r) = i_1 \tag{14}$$

and fixes (that is, leaves unchanged) the other numbers in $\{1, 2, \ldots, n\}$ is called a *cycle* or an *r-cycle*. We denote this as

$$\gamma = (i_1 i_2 \cdots i_r). \tag{15}$$

It is clear that we can equally well write

$$\gamma = (i_2 i_3 \cdots i_r i_1) = (i_3 i_4 \cdots i_r i_1 i_2), \text{ etc.}$$

The permutation γ^2 maps i_1 into i_3, i_2 into $i_4, \ldots, i_r$ into i_2 etc., and, in general, for $1 \leq k \leq r$,

$$\begin{aligned} \gamma^k(i_j) &= i_{j+k} \quad \text{if} \quad j + k \leq r \\ \gamma^k(i_j) &= i_{j+k-r} \quad \text{if} \quad j + k > r. \end{aligned} \tag{16}$$

Clearly this shows that $\gamma^r = 1$ but $\gamma^k \neq 1$ if $1 \leq k < r$. Hence γ is of order r.

Two cycles γ and γ' are said to be *disjoint* if their symbols contain no common letters. In this case it is clear that any number moved by one of these transformations is fixed by the other. Hence if i is any number such that $\gamma(i) \neq i$ then $\gamma\gamma'(i) = \gamma(i)$, and since also $\gamma^2(i) \neq \gamma(i)$, $\gamma'\gamma(i) = \gamma(i)$. Similarly, if $\gamma'(i) \neq i$ then $\gamma'\gamma(i) = \gamma'(i) = \gamma\gamma'(i)$. Also if $\gamma(i) = i = \gamma'(i)$ then $\gamma\gamma'(i) = \gamma'\gamma(i)$. Thus $\gamma\gamma' = \gamma'\gamma$, that is, any two disjoint cycles commute. Let α be a product of disjoint cycles, that is,

$$\alpha = (i_1 i_2 \cdots i_r)(j_1 j_2 \cdots j_s) \cdots (l_1 l_2 \cdots l_u). \tag{17}$$

Let m be the least common multiple of $r, s, \ldots, u$. Then we claim that m is the order of α. Putting $\gamma_1 = (i_1 \cdots i_r)$, $\gamma_2 = (j_1 \cdots j_s), \ldots, \gamma_k = (l_1 \cdots l_u)$ we have $\alpha^m = \gamma_1^m \gamma_2^m \cdots \gamma_k^m = 1$. On the other hand, α permutes $i_1, \ldots, i_r$ and so do its powers and the restriction of α to $\{i_1, \ldots, i_r\}$ is γ_1. Hence if $\alpha^n = 1$ then $\gamma_1^n =$

1 and so n is divisible by r. Similarly, n is divisible by $s, \ldots, u$ and so n is divisible by the least common multiple of $r, s, \ldots, u$. Hence the least common multiple of these numbers is the order of α.

It is convenient to extend the definition of cycles and the cycle notation to 1-cycles where we adopt the convention that for any i, (i) is the identity mapping. With this convention we can see that every permutation is a product of disjoint cycles. For example, if

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

then

$$\alpha(1) = 3, \alpha(3) = 5, \alpha(5) = 8, \alpha(8) = 1; \alpha(2) = 6, \alpha(6) = 2; \alpha(4) = 4, \alpha(7) = 7$$

from which one deduces that

$$\alpha = (7)(4)(26)(1358).$$

In general, for any α we can begin with any number in $1, 2, \ldots, n$, say i_1, and form $\alpha(i_1) = i_2, \alpha(i_2) = i_3, \ldots$, until we reach a number that occurs previously in this list. The first such repetition occurs when $i_{r+1} = \alpha(i_r) = i_1$; for, we have $i_k = \alpha^{k-1}(i_1)$ and if $i_k = i_l$ for $l > k$ then $\alpha^{l-k}(i_1) = i_1$. Thus the sequence $i_1, i_2, \ldots, i_r$ is permuted cyclically by α. If $r < n$ we choose a j_1 not in $\{i_1, i_2, \ldots, i_r\}$. If $\alpha^m(j_1) = \alpha^q(i_1)$ then $j_1 = \alpha^{q-m}(i_1) \in \{i_1, i_2, \ldots, i_r\}$ contrary to our choice of j_1. Hence we obtain a new sequence of numbers $j_1, j_2, \ldots, j_s$ permuted cyclically by α and having no elements in common with the first. Continuing in this way we ultimately exhaust the set $\{1, 2, \ldots, n\}$. It is clear, on comparing the images of any i under the two maps α and $(l_1 \cdots l_u) \cdots (i_1 \cdots i_r)$ that

$$\alpha = (l_1 \cdots l_u) \cdots (i_1 \cdots i_r),$$

a product of disjoint cycles. The different cycles occurring in such a factorization commute and we may add or drop trivial one-cycles. Apart from order of the factors and inclusion or omission of 1-cycles this factorization is unique. For, if we have one which is essentially different from the one displayed above (or 17)), then for some i, j, $i \neq j$, which occur in the order i followed by j in one of the cycles in (17), we have that this is not the case in the other one. The first factorization then shows that $\alpha(i) = j$ and the second that $\alpha(i) \neq j$. This contradiction proves our assertion.

A cycle of the form (ab) is called a *transposition*. It is easy to verify that

$$(i_1 i_2 \cdots i_r) = (i_1 i_r) \cdots (i_1 i_3)(i_1 i_2), \tag{18}$$

a product of $r-1$ transpositions. It follows that any $\alpha \in S_n$ is a product of transpositions. In fact, if α factors as a product of disjoint cycles as in (17), then α is a product of $(r-1)+(s-1)+\cdots+(u-1)$ transpositions. We denote this number, which is uniquely determined by α, as $N(\alpha)$. It is clear that $N(1)=0$. There is no uniqueness of factorization of a permutation as a product of transpositions. For example, we have $(123)=(13)(12)=(12)(23)=(23)(13)$. However, as we shall now show, there is one common feature of all the factorizations of a given α as a product of transpositions. The number of factors occurring all have the same parity: that is, their number is either always even or always odd. Our proof of this fact will be based on a simple formula, which is anyhow worth noting:

$$(ab)(ac_1\cdots c_h bd_1\cdots d_k)=(bd_1\cdots d_k)(ac_1\cdots c_h). \tag{19}$$

Here we are allowing h or k to be 0, meaning thereby that no c's or no d's occur. Comparing images of any i in $\{1, 2, \ldots, n\}$ shows that (19) holds. Since $(ab)^{-1}=(ab)$ multiplying both sides of (19) on the left by (ab) gives:

$$(ab)(bd_1\cdots d_k)(ac_1\cdots c_h)=(ac_1\cdots c_h bd_1\cdots d_k). \tag{20}$$

If N is defined as above, we have $N((ac_1\cdots c_h bd_1\cdots d_k))=h+k+1$ and $N((bd_1\cdots d_k)(ac_1\cdots c_h))=h+k$. It follows that $N((ab)(\alpha))=N(\alpha)-1$ if a and b occur in the same cycle in the decomposition of α into disjoint cycles and $N((ab)\alpha)=N(\alpha)+1$ if a and b occur in different cycles. Hence if α is a product of m transpositions then, since $N(1)=0$, $N(\alpha)=\sum_{i=1}^{m}\varepsilon_i$ where $\varepsilon_i=\pm 1$. Changing an $\varepsilon_i=-1$ to 1 amounts to adding 2 to the sum and so does not change the parity. If we make this change for every $\varepsilon_i=-1$ the final sum we obtain is m. Hence m and $N(\alpha)$ have the same parity. Hence the number of factors in any two factorizations of α as a product of transpositions have the same parity, namely, the parity of $N(\alpha)$.

We call α *even* or *odd* according as α factors as a product of an even or an odd number of transpositions (equivalently: $N(\alpha)$ is even or odd.) We define the *sign* of α, $sg\ \alpha$, by

$$sg\ \alpha = 1 \text{ if } \alpha \text{ is even}, \qquad sg\ \alpha = -1 \text{ if } \alpha \text{ is odd} \tag{21}$$

Then $sg\ 1=1$ and if $\alpha=(ab)\cdots(kl)$, $\beta=(pq)\cdots(uv)$, $\alpha\beta=(ab)\cdots(kl)(pq)\cdots(uv)$. Hence $\alpha\beta$ is even if and only if both α and β are even or both are odd while $\alpha\beta$ is odd if one of the factors is even and the other is odd. It follows that

$$sg\ \alpha\beta=(sg\ \alpha)(sg\ \beta). \tag{22}$$

It is clear also that the subset A_n of even permutations is a subgroup of S_n.

This is called the *alternating group* (of degree n). Suppose we list its elements as

$$\alpha_1, \alpha_2, \ldots, \alpha_m.$$

Then if $n \geq 2$ we have m different odd permutations

$$\alpha_1(ab), \alpha_2(ab), \ldots, \alpha_m(ab)$$

and this catches them all, since if β is odd $\beta(ab)$ is even so $\beta(ab)=\alpha_i$ for some i and $\beta=\alpha_i(ab)$. Hence $|S_n|=2m=2|A_n|$ and so $|A_n|=n!/2$ if $n \geq 2$.

EXERCISES

1. Write $(456)(567)(671)(123)(234)(345)$ as a product of disjoint cycles.
2. Show that if $n \geq 3$ then A_n is generated by the 3-cycles (abc).
3. Determine the sign of the permutation
$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}.$$
4. Show that if α is any permutation then
$$\alpha(i_1 i_2\cdots i_r)\alpha^{-1}=(\alpha(i_1)\alpha(i_2)\cdots\alpha(i_r)).$$
5. Show that S_n is generated by the $n-1$ transpositions $(12), (13), \ldots, (1n)$ and also by the $n-1$ transpositions $(12), (23), \ldots, (n-1n)$.

1.7 ORBITS. COSETS OF A SUBGROUP

Let G be a group of transformations of a set S. Then G defines an equivalence relation on S by the rule that $x \sim_G y$ (read: x is *G-equivalent* to y) if $y=\alpha(x)$ for some $\alpha \in G$. That this relation is reflexive, symmetric, and transitive is immediate from the definition of a transformation group: $x=1_S(x)$, also if $y=\alpha(x)$ then $x=\alpha^{-1}(y)$, and if $y=\alpha(x)$ and $z=\beta(y)$ then $z=(\beta\alpha)(x)$. Moreover, $1_S \in G$ and α^{-1} and $\beta\alpha \in G$, if α and $\beta \in G$. The G-equivalence class determined by an element x is the set $Gx=\{\alpha(x)|\alpha \in G\}$ and this is called the *G-orbit* of $x \in S$. For example, if G is the group of rotations about the origin in a plane, then the orbit of a point P is the circle through P with center at the origin. As with any equivalence relation, the set of orbits constitute a partition of the set S. It may happen that there is just one orbit, that is, $S=Gx$ for some x (and hence for every x). In this case we say that G is a *transitive* group of transformations