for all $g \in G$ and all $a \in A$. The kernel of this action is the same as $\ker \varphi$. The permutation representation associated to this action is precisely the given homomorphism φ. This proves the following result.

Proposition 1. For any group G and any nonempty set A there is a bijection between the actions of G on A and the homomorphisms of G into S_A.

In view of Proposition 1 the definition of a permutation representation may be rephrased.

Definition. If G is a group, a *permutation representation* of G is any homomorphism of G into the symmetric group S_A for some nonempty set A. We shall say a given action of G on A *affords* or *induces* the associated permutation representation of G.

We can think of a permutation representation as an analogue of the matrix representation of a linear transformation. In the case where A is a finite set of n elements we have $S_A \cong S_n$ (cf. Section 1.6), so by fixing a labelling of the elements of A we may consider our permutations as elements of the group S_n (which is exactly what we did in Examples 2 and 3 above), in the same way that fixing a basis for a vector space allows us to view a linear transformation as a matrix.

We now prove a combinatorial result about group actions which will have important consequences when we apply it to specific actions in subsequent sections.

Proposition 2. Let G be a group acting on the nonempty set A. The relation on A defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.

Proof: We first prove $\sim$ is an equivalence relation. By axiom 2 of an action, $a = 1 \cdot a$ for all $a \in A$, i.e., $a \sim a$ and the relation is reflexive. If $a \sim b$, then $a = g \cdot b$ for some $b \in G$ so that

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = 1 \cdot b = b$$

that is, $b \sim a$ and the relation is symmetric. Finally, if $a \sim b$ and $b \sim c$, then $a = g \cdot b$ and $b = h \cdot c$, for some $g, h \in G$ so

$$a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c$$

hence $a \sim c$, and the relation is transitive.

To prove the last statement of the proposition we exhibit a bijection between the left cosets of G_a in G and the elements of the equivalence class of a. Let $\mathcal{C}_a$ be the class of a, so

$$\mathcal{C}_a = \{g \cdot a \mid g \in G\}.$$

Suppose $b = g \cdot a \in \mathcal{C}_a$. Then gG_a is a left coset of G_a in G. The map

$$b = g \cdot a \mapsto gG_a$$

is a map from $\mathcal{C}_a$ to the set of left cosets of G_a in G. This map is surjective since for any $g \in G$ the element $g \cdot a$ is an element of $\mathcal{C}_a$. Since $g \cdot a = h \cdot a$ if and only if $h^{-1}g \in G_a$ if and only if $gG_a = hG_a$, the map is also injective, hence is a bijection. This completes the proof.

By Proposition 2 a group G acting on the set A partitions A into disjoint equivalence classes under the action of G. These classes are given a name:

Definition. Let G be a group acting on the nonempty set A.

(1) The equivalence class $\{g \cdot a \mid g \in G\}$ is called the *orbit* of G containing a.

(2) The action of G on A is called *transitive* if there is only one orbit, i.e., given any two elements $a, b \in A$ there is some $g \in G$ such that $a = g \cdot b$.

Examples

Let G be a group acting on the set A.

(1) If G acts trivially on A then $G_a = G$ for all $a \in A$ and the orbits are the elements of A. This action is transitive if and only if $|A| = 1$.

(2) The symmetric group $G = S_n$ acts transitively in its usual action as permutations on $A = \{1, 2, \ldots, n\}$. Note that the stabilizer in G of any point i has index $n = |A|$ in S_n.

(3) When the group G acts on the set A, any subgroup of G also acts on A. If G is transitive on A a subgroup of G need not be transitive on A. For example, if $G = \langle (1\ 2), (3\ 4) \rangle \leq S_4$ then the orbits of G on $\{1, 2, 3, 4\}$ are $\{1, 2\}$ and $\{3, 4\}$ and there is no element of G that sends 2 to 3. The discussion below on cycle decompositions shows that when $\langle \sigma \rangle$ is any cyclic subgroup of S_n then the orbits of $\langle \sigma \rangle$ consist of the sets of numbers that appear in the individual cycles in the cycle decomposition of σ (for example, the orbits of $\langle (1\ 2)(3\ 4\ 5) \rangle$ are $\{1, 2\}$ and $\{3, 4, 5\}$).

(4) The group D_8 acts transitively on the four vertices of the square and the stabilizer of any vertex is the subgroup of order 2 (and index 4) generated by the reflection about the line of symmetry passing through that point.

(5) The group D_8 also acts transitively on the set of two pairs of opposite vertices. In this action the stabilizer of any point is $\langle s, r^2 \rangle$ (which is of index 2).

Cycle Decompositions

We now prove that every element of the symmetric group S_n has the unique cycle decomposition described in Section 1.3. Let $A = \{1, 2, \ldots, n\}$, let σ be an element of S_n and let $G = \langle \sigma \rangle$. Then $\langle \sigma \rangle$ acts on A and so, by Proposition 2, it partitions $\{1, 2, \ldots, n\}$ into a unique set of (disjoint) orbits. Let $\mathcal{O}$ be one of these orbits and let $x \in \mathcal{O}$. By (the proof of) Proposition 2 applied to $A = \mathcal{O}$ we see that there is a bijection between the left cosets of G_x in G and the elements of $\mathcal{O}$, given explicitly by

$$\sigma^i x \mapsto \sigma^i G_x.$$

Since G is a cyclic group, $G_x \trianglelefteq G$ and G/G_x is cyclic of order d, where d is the smallest positive integer for which $\sigma^d \in G_x$ (cf. Example 2 following Proposition 7 in Section 3.1). Also, $d = |G : G_x| = |\mathcal{O}|$. Thus the distinct cosets of G_x in G are

$$1G_x,\ \sigma G_x,\ \sigma^2 G_x,\ \ldots,\ \sigma^{d-1} G_x.$$

This shows that the distinct elements of $\mathcal{O}$ are

$$x,\ \sigma(x),\ \sigma^2(x),\ \ldots,\ \sigma^{d-1}(x).$$

Ordering the elements of $\mathcal{O}$ in this manner shows that σ cycles the elements of $\mathcal{O}$, that is, on an orbit of size d, σ acts as a d-cycle. This proves the existence of a cycle decomposition for each $\sigma \in S_n$.

The orbits of $\langle \sigma \rangle$ are uniquely determined by σ. The only latitude is in which order the orbits are listed. Within each orbit, $\mathcal{O}$, we may begin with any element as a representative. Choosing $\sigma^i(x)$ instead of x as the initial representative simply produces the elements of $\mathcal{O}$ in the order

$$\sigma^i(x),\ \sigma^{i+1}(x),\ \ldots,\ \sigma^{d-1}(x),\ x,\ \sigma(x),\ \ldots,\ \sigma^{i-1}(x),$$

which is a cyclic permutation (forward $i-1$ terms) of the original list. It follows that the cycle decomposition above is unique up to a rearrangement of the cycles and up to a cyclic permutation of the integers within each cycle.

Subgroups of symmetric groups are called *permutation groups*. For any subgroup G of S_n the orbits of G will refer to its orbits on $\{1, 2, \ldots, n\}$. The orbits of an element σ in S_n will mean the orbits of the group $\langle \sigma \rangle$ (namely the sets of integers comprising the cycles in its cycle decomposition).

The exercises below further illustrate how group theoretic information can be obtained from permutation representations.

EXERCISES

Let G be a group and let A be a nonempty set.

1. Let G act on the set A. Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$ (G_a is the stabilizer of a). Deduce that if G acts transitively on A then the kernel of the action is $\cap_{g \in G}\, gG_ag^{-1}$.
2. Let G be a *permutation group* on the set A (i.e., $G \leq S_A$), let $\sigma \in G$ and let $a \in A$. Prove that $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$. Deduce that if G acts transitively on A then

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1.$$

3. Assume that G is an abelian, transitive subgroup of S_A. Show that $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$. Deduce that $|G| = |A|$. [Use the preceding exercise.]
4. Let S_3 act on the set Ω of ordered pairs: $\{(i, j) \mid 1 \leq i, j \leq 3\}$ by $\sigma((i, j)) = (\sigma(i), \sigma(j))$. Find the orbits of S_3 on Ω. For each $\sigma \in S_3$ find the cycle decomposition of σ under this action (i.e., find its cycle decomposition when σ is considered as an element of S_9 — first fix a labelling of these nine ordered pairs). For each orbit $\mathcal{O}$ of S_3 acting on these nine points pick some $a \in \mathcal{O}$ and find the stabilizer of a in S_3.
5. For each of parts (a) and (b) repeat the preceding exercise but with S_3 acting on the specified set:
   (a) the set of 27 triples $\{(i, j, k) \mid 1 \leq i, j, k \leq 3\}$
   (b) the set $\mathcal{P}(\{1, 2, 3\}) - \{\emptyset\}$ of all 7 nonempty subsets of $\{1, 2, 3\}$.
6. As in Exercise 12 of Section 2.2 let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 and let S_4 act on R by permuting the indices of