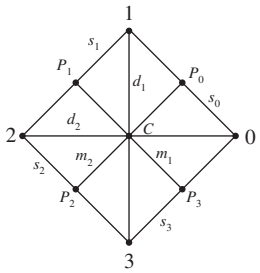

14.10 Figure

We can think of the set

$$X = \{0, 1, 2, 3, s_0, s_1, s_2, s_3, m_1, m_2, d_1, d_2, C, P_0, P_1, P_2, P_3\}$$

as a D_4-set in a natural way. Table 14.11 shows the action of D_4 on X. Recall that ι is the identity, ρ^k is rotation by $k\pi/2$, and μ is reflection across the line d_2. We can see from the table that $\mu\rho$ is reflection across the line m_1, $\mu\rho^2$ is reflection across the line d_1, and $\mu\rho^3$ is reflection across the line m_2. It is worthwhile to spend a little time to understand how Table 14.11 was constructed before continuing. ▲

14.11 Table

	0	1	2	3	s_0	s_1	s_2	s_3	m_1	m_2	d_1	d_2	C	P_0	P_1	P_2	P_3
ι	0	1	2	3	s_0	s_1	s_2	s_3	m_1	m_2	d_1	d_2	C	P_0	P_1	P_2	P_3
ρ	1	2	3	0	s_1	s_2	s_3	s_0	m_2	m_1	d_2	d_1	C	P_1	P_2	P_3	P_0
ρ^2	2	3	0	1	s_2	s_3	s_0	s_1	m_1	m_2	d_1	d_2	C	P_2	P_3	P_0	P_1
ρ^3	3	0	1	2	s_3	s_0	s_1	s_2	m_2	m_1	d_2	d_1	C	P_3	P_0	P_1	P_2
μ	0	3	2	1	s_3	s_2	s_1	s_0	m_2	m_1	d_1	d_2	C	P_3	P_2	P_1	P_0
$\mu\rho$	3	2	1	0	s_2	s_1	s_0	s_3	m_1	m_2	d_2	d_1	C	P_2	P_1	P_0	P_3
$\mu\rho^2$	2	1	0	3	s_1	s_0	s_3	s_2	m_2	m_1	d_1	d_2	C	P_1	P_0	P_3	P_2
$\mu\rho^3$	1	0	3	2	s_0	s_3	s_2	s_1	m_1	m_2	d_2	d_1	C	P_0	P_3	P_2	P_1

Isotropy Subgroups

Let X be a G-set. Let $x \in X$ and $g \in G$. It will be important to know when $gx = x$. We let

$$X_g = \{x \in X \mid gx = x\} \qquad \text{and} \qquad G_x = \{g \in G \mid gx = x\}.$$

14.12 Example For the D_4-set X in Example 14.9, we have

$$X_\iota = X, \qquad X_\rho = \{C\}, \qquad X_\mu = \{0, 2, d_1, d_2, C\}.$$

Also, using the same D_4 action on X,

$$G_0 = \{\iota, \mu\}, \qquad G_{s_2} = \{\iota, \mu\rho^3\}, \qquad G_{d_1} = \{\iota, \rho^2, \mu, \mu\rho^2\}.$$

We leave the computations of the other sets of the form X_σ and G_x to Exercises 1 and 2. ▲

Note that the subsets G_x given in the preceding example were, in each case, subgroups of G. This is true in general.

14.13 Theorem Let X be a G-set. Then G_x is a subgroup of G for each $x \in X$.

Proof Let $x \in X$ and let $g_1, g_2 \in G_x$. Then $g_1x = x$ and $g_2x = x$. Consequently, $(g_1g_2)x = g_1(g_2x) = g_1x = x$, so $g_1g_2 \in G_x$, and G_x is closed under the induced operation of G. Of course, $ex = x$, so $e \in G_x$. If $g \in G_x$, then $gx = x$, so $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$, and consequently $g^{-1} \in G_x$. Thus G_x is a subgroup of G. ◆

14.14 Definition Let X be a G-set and let $x \in X$. The subgroup G_x is the **isotropy subgroup of** x. ■

Orbits

For the D_4-set X of Example 14.9 with action table in Table 14.11, the elements in the subset {0, 1, 2, 3} are carried into elements of this same subset under action by D_4. Furthermore, each of the elements 0, 1, 2, and 3 is carried into all the other elements of the subset by the various elements of D_4. We proceed to show that every G-set X can be partitioned into subsets of this type.

14.15 Theorem Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

Proof For each $x \in X$, we have $ex = x$, so $x \sim x$ and $\sim$ is reflexive.

Suppose $x_1 \sim x_2$, so $gx_1 = x_2$ for some $g \in G$. Then $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1$, so $x_2 \sim x_1$, and $\sim$ is symmetric.

Finally, if $x_1 \sim x_2$ and $x_2 \sim x_3$, then $g_1x_1 = x_2$ and $g_2x_2 = x_3$ for some $g_1, g_2 \in G$. Then $(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$, so $x_1 \sim x_3$ and $\sim$ is transitive. ◆

14.16 Definition Let X be a G-set. Each cell in the partition of the equivalence relation described in Theorem 14.15 is an **orbit in** X **under** G. If $x \in X$, the cell containing x is the **orbit of** x. We let this cell be Gx. ■

The relationship between the orbits in X and the group structure of G lies at the heart of many applications. The following theorem gives this relationship. Recall that for a set X, we use $|X|$ for the number of elements in X, and $(G : H)$ is the index of a subgroup H in a group G.

14.17 Theorem Let X be a G-set and let $x \in X$. Then $|Gx| = (G : G_x)$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.

Proof We define a one-to-one map ψ from Gx onto the collection of left cosets of G_x in G. Let $x_1 \in Gx$. Then there exists $g_1 \in G$ such that $g_1x = x_1$. We define $\psi(x_1)$ to be the left coset g_1G_x of G_x. We must show that this map ψ is well defined, independent of the choice of $g_1 \in G$ such that $g_1x = x_1$. Suppose also that $g_1'x = x_1$. Then, $g_1x = g_1'x$, so $g_1^{-1}(g_1x) = g_1^{-1}(g_1'x)$, from which we deduce $x = (g_1^{-1}g_1')x$. Therefore $g_1^{-1}g_1' \in G_x$, so $g_1' \in g_1G_x$, and $g_1G_x = g_1'G_x$. Thus the map ψ is well defined.

To show the map ψ is one-to-one, suppose $x_1, x_2 \in Gx$, and $\psi(x_1) = \psi(x_2)$. Then there exist $g_1, g_2 \in G$ such that $x_1 = g_1x, x_2 = g_2x$, and $g_2 \in g_1G_x$. Then $g_2 = g_1g$ for some $g \in G_x$, so $x_2 = g_2x = g_1(gx) = g_1x = x_1$. Thus ψ is one-to-one.

Finally, we show that each left coset of G_x in G is of the form $\psi(x_1)$ for some $x_1 \in Gx$. Let g_1G_x be a left coset. Then if $g_1x = x_1$, we have $g_1G_x = \psi(x_1)$. Thus ψ maps Gx one-to-one onto the collection of left cosets so $|Gx| = (G : G_x)$.

If $|G|$ is finite, then the equation $|G| = |G_x|(G : G_x)$ shows that $|Gx| = (G : G_x)$ is a divisor of $|G|$. ◆

14.18 Example Let X be the D_4-set in Example 14.9, with action table given by Table 14.11. With $G = D_4$, we have $G_0 = \{\iota, \mu\}$. Since $|G| = 8$, we have $|G0| = (G : G_0) = 4$. From Table 14.11, we see that $G0 = \{0, 1, 2, 3\}$, which indeed has four elements. ▲

We should remember not only the cardinality equation in Theorem 14.17 but also that the *elements of G carrying x into g_1x are precisely the elements of the left coset g_1G_x*. Namely, if $g \in G_x$, then $(g_1g)x = g_1(gx) = g_1x$. On the other hand, if $g_2x = g_1x$, then $g_1^{-1}(g_2x) = x$ so $(g_1^{-1}g_2)x = x$. Thus $g_1^{-1}g_2 \in G_x$ so $g_2 \in g_1G_x$.

Applications of G-Sets to Finite Groups

Theorem 14.17 is a very useful theorem in the study of finite groups. Suppose that X is a G-set for a finite group G and we pick out one element from each orbit of X to make the set $S = \{x_1, x_2, \ldots, x_r\}$ where we indexed the elements of X so that if $i \leq j$, then $|Gx_i| \geq |Gx_j|$. That is, we arrange by orbit size, largest first and smallest last. Every element in X is in precisely one orbit, so

$$|X| = \sum_{i=1}^{r} |Gx_i|. \tag{1}$$

We let $X_G = \{x \in X \mid gx = x \text{ for all } g \in G\}$. That is, X_G is the set of all elements of X whose orbit size is 1. So by equation (1),

$$|X| = |X_G| + \sum_{i=1}^{s} |Gx_i| \tag{2}$$

where we simply place all the orbits with one element into X_G and we are left with s orbits each containing at least two elements. Although Equation (2) is simply saying that if you add up the sizes of all the orbits you account for all the elements of X, when coupled with Theorem 14.17, it gives some very interesting results. We give a few in the remainder of this section. In Section 17 we will use Equation 2 extensively to prove the Sylow Theorems.

For the remainder of this section, *we assume that p is a prime number*.

14.19 Theorem Let G be a group with p^n elements. If X is a G-set, then $|X| \equiv |X_G| \mod p$.

Proof Using Equation 2,

$$|X| = |X_G| + \sum_{i=1}^{s} |Gx_i|.$$

Since for each $i \leq s$, $|Gx_i| \geq 2$ and $|Gx_i| = (G : G_{x_i})$ is a divisor of $|G| = p^n$, by Theorem 14.17 p divides each term in the sum $\sum_{i=1}^{s} |Gx_i|$. Thus $|X| \equiv |X_G| \mod p$. ◆

Knowing that k divides the order of a group is not sufficient information to assume that the group has a subgroup of order k. For example, we saw that A_4 has no subgroup of order 6 and that in general, A_n has no subgroup of index 2 if $n \geq 4$. On the positive side, in Exercise 29 in Section 2, you were asked to show that if a group has an even number of elements, then it has an element of order two. Theorem 14.20 generalizes this result to show that if a prime number p divides the order of a group, then the group has an element of order p. The proof of this theorem relies on Theorem 14.19.

14.20 Theorem **(Cauchy's Theorem)** Let G be a group such that p divides the order of G. Then G has an element of order p and therefore a subgroup of order p.