**Examples**

**(1)** The group $G = D_8$ acts on the set $A$ of four vertices of a square (cf. Example 4 in Section 1.7). The stabilizer of any vertex $a$ is the subgroup $\{1, t\}$ of $D_8$, where $t$ is the reflection about the line of symmetry passing through vertex $a$ and the center of the square. The kernel of this action is the identity subgroup since only the identity symmetry fixes every vertex.

**(2)** The group $G = D_8$ also acts on the set $A$ whose elements are the two unordered pairs of opposite vertices (in the labelling of Figure 2 in Section 1.2, $A = \{\{1, 3\}, \{2, 4\}\}$). The kernel of the action of $D_8$ on this set $A$ is the subgroup $\{1, s, r^2, sr^2\}$ and for either element $a \in A$ the stabilizer of $a$ in $D_8$ equals the kernel of the action.

Finally, we observe that the fact that centralizers, normalizers and kernels are subgroups is a special case of the facts that stabilizers and kernels of actions are subgroups (this will be discussed further in Chapter 4). Let $S = \mathcal{P}(G)$, the collection of all subsets of $G$, and let $G$ act on $S$ by *conjugation*, that is, for each $g \in G$ and each $B \subseteq G$ let

$$g : B \to gBg^{-1} \quad \text{where} \quad gBg^{-1} = \{gbg^{-1} \mid b \in B\}$$

(see Exercise 16 in Section 1.7). Under this action, it is easy to check that $N_G(A)$ is precisely the stabilizer of $A$ in $G$ (i.e., $N_G(A) = G_s$ where $s = A \in \mathcal{P}(G)$), so $N_G(A)$ is a subgroup of $G$.

Next let the group $N_G(A)$ act on the set $S = A$ by conjugation, i.e., for all $g \in N_G(A)$ and $a \in A$

$$g : a \mapsto gag^{-1}.$$

Note that this does map $A$ to $A$ by the definition of $N_G(A)$ and so gives an action on $A$. Here it is easy to check that $C_G(A)$ is precisely the kernel of this action, hence $C_G(A) \leq N_G(A)$; by transitivity of the relation "$\leq$," $C_G(A) \leq G$. Finally, $Z(G)$ is the kernel of $G$ acting on $S = G$ by conjugation, so $Z(G) \leq G$.

## EXERCISES

**1.** Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

**2.** Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

**3.** Prove that if $A$ and $B$ are subsets of $G$ with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

**4.** For each of $S_3$, $D_8$, and $Q_8$ compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem (Exercise 19 in Section 1.7) simplify your work?

**5.** In each of parts (a) to (c) show that for the specified group $G$ and subgroup $A$ of $G$, $C_G(A) = A$ and $N_G(A) = G$.
- **(a)** $G = S_3$ and $A = \{1, (1\,2\,3), (1\,3\,2)\}$.
- **(b)** $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.
- **(c)** $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

**6.** Let $H$ be a subgroup of the group $G$.
- **(a)** Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if $H$ is not a subgroup.
- **(b)** Show that $H \leq C_G(H)$ if and only if $H$ is abelian.

**7.** Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:
- **(a)** $Z(D_{2n}) = 1$ if $n$ is odd

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

**8.** Let G = $S_n$, fix an $i \in \{1, 2, \ldots, n\}$ and let $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ (the stabilizer of $i$ in $G$). Use group actions to prove that $G_i$ is a subgroup of $G$. Find $|G_i|$.

**9.** For any subgroup $H$ of $G$ and any nonempty subset $A$ of $G$ define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of $H$ (note that $A$ need not be a subset of $H$).

**10.** Let $H$ be a subgroup of order 2 in $G$. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

**11.** Prove that $Z(G) \leq N_G(A)$ for any subset $A$ of $G$.

**12.** Let $R$ be the set of all polynomials with integer coefficients in the independent variables $x_1, x_2, x_3, x_4$ i.e., the members of $R$ are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$, where $a$ is any integer and $r_1, \ldots, r_4$ are nonnegative integers. For example,

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23} \qquad (*)$$

is a typical element of $R$. Each $\sigma \in S_4$ gives a permutation of $\{x_1, \ldots, x_4\}$ by defining $\sigma \cdot x_i = x_{\sigma(i)}$. This may be extended to a map from $R$ to $R$ by defining

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

for all $p(x_1, x_2, x_3, x_4) \in R$ (i.e., $\sigma$ simply permutes the indices of the variables). For example, if $\sigma = (1\ 2)(3\ 4)$ and $p(x_1, \ldots, x_4)$ is the polynomial in $(*)$ above, then

$$\begin{aligned}\sigma \cdot p(x_1, x_2, x_3, x_4) &= 12x_2^5x_1^7x_3 - 18x_1^3x_4 + 11x_2^6x_1x_4^3x_3^{23} \\ &= 12x_1^7x_2^5x_3 - 18x_1^3x_4 + 11x_1x_2^6x_3^{23}x_4^3.\end{aligned}$$

(a) Let $p = p(x_1, \ldots, x_4)$ be the polynomial in $(*)$ above, let $\sigma = (1\ 2\ 3\ 4)$ and let $\tau = (1\ 2\ 3)$. Compute $\sigma \cdot p$, $\tau \cdot (\sigma \cdot p)$, $(\tau \circ \sigma) \cdot p$, and $(\sigma \circ \tau) \cdot p$.

(b) Prove that these definitions give a (left) group action of $S_4$ on $R$.

(c) Exhibit all permutations in $S_4$ that stabilize $x_4$ and prove that they form a subgroup isomorphic to $S_3$.

(d) Exhibit all permutations in $S_4$ that stabilize the element $x_1 + x_2$ and prove that they form an abelian subgroup of order 4.

(e) Exhibit all permutations in $S_4$ that stabilize the element $x_1x_2 + x_3x_4$ and prove that they form a subgroup isomorphic to the dihedral group of order 8.

(f) Show that the permutations in $S_4$ that stabilize the element $(x_1 + x_2)(x_3 + x_4)$ are exactly the same as those found in part (e). (The two polynomials appearing in parts (e) and (f) and the subgroup that stabilizes them will play an important role in the study of roots of quartic equations in Section 14.6.)

**13.** Let $n$ be a positive integer and let $R$ be the set of all polynomials with integer coefficients in the independent variables $x_1, x_2, \ldots, x_n$, i.e., the members of $R$ are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$, where $a$ is any integer and $r_1, \ldots, r_n$ are nonnegative integers. For each $\sigma \in S_n$ define a map

$$\sigma : R \to R \qquad \text{by} \qquad \sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Prove that this defines a (left) group action of $S_n$ on $R$.

**14.** Let $H(F)$ be the Heisenberg group over the field $F$ introduced in Exercise 11 of Section 1.4. Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group $F$.

## 2.3 CYCLIC GROUPS AND CYCLIC SUBGROUPS

Let $G$ be any group and let $x$ be any element of $G$. One way of forming a subgroup $H$ of $G$ is by letting $H$ be the set of all integer (positive, negative and zero) powers of $x$ (this guarantees closure under inverses and products at least as far as $x$ is concerned). In this section we study groups which are generated by one element.

**Definition.** A group $H$ is *cyclic* if $H$ can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).

In additive notation $H$ is cyclic if $H = \{ nx \mid n \in \mathbb{Z}\}$. In both cases we shall write $H = \langle x \rangle$ and say $H$ is *generated* by $x$ (and $x$ is a *generator* of $H$). A cyclic group may have more than one generator. For example, if $H = \langle x \rangle$, then also $H = \langle x^{-1} \rangle$ because $(x^{-1})^n = x^{-n}$ and as $n$ runs over all integers so does $-n$ so that

$$\{x^n \mid n \in \mathbb{Z}\} = \{(x^{-1})^n \mid n \in \mathbb{Z}\}.$$

We shall shortly show how to determine all generators for a given cyclic group $H$. One should note that the elements of $\langle x \rangle$ are powers of $x$ (or multiples of $x$, in groups written additively) and not integers. It is not necessarily true that all powers of $x$ are distinct. Also, by the laws for exponents (Exercise 19 in Section 1.1) cyclic groups are abelian.

**Examples**

**(1)** Let $G = D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$, $n \geq 3$ and let $H$ be the subgroup of all rotations of the $n$-gon. Thus $H = \langle r \rangle$ and the distinct elements of $H$ are $1, r, r^2, \ldots, r^{n-1}$ (these are all the distinct powers of $r$). In particular, $|H| = n$ and the generator, $r$, of $H$ has order $n$. The powers of $r$ "cycle" (forward and backward) with period $n$, that is,

$$r^n = 1,\ r^{n+1} = r,\ r^{n+2} = r^2, \ldots$$
$$r^{-1} = r^{n-1},\ r^{-2} = r^{n-2}, \ldots \quad \text{etc.}$$

In general, to write any power of $r$, say $r^t$, in the form $r^k$, for some $k$ between 0 and $n-1$ use the Division Algorithm to write

$$t = nq + k, \qquad \text{where } 0 \leq k < n,$$

so that

$$r^t = r^{nq+k} = (r^n)^q r^k = 1^q r^k = r^k.$$

For example, in $D_8$, $r^4 = 1$ so $r^{105} = r^{4(26)+1} = r$ and $r^{-42} = r^{4(-11)+2} = r^2$. Observe that $D_{2n}$ itself is not a cyclic group since it is non-abelian.

**(2)** Let $H = \mathbb{Z}$ with operation $+$. Thus $H = \langle 1 \rangle$ (here 1 is the integer 1 and the identity of $H$ is 0) and each element in $H$ can be written uniquely in the form $n \cdot 1$, for some $n \in \mathbb{Z}$. In contrast to the preceding example, multiples of the generator are all distinct and we need to take both positive, negative and zero multiples of the generator to obtain all elements of $H$. In this example $|H|$ and the order of the generator 1 are both $\infty$. Note also that $H = \langle -1 \rangle$ since each integer $x$ can be written (uniquely) as $(-x)(-1)$.

Before discussing cyclic groups further we prove that the various properties of finite and infinite cyclic groups we observed in the preceding two examples are generic. This proposition also validates the claim (in Chapter 1) that the use of the terminology for "order" of an element and the use of the symbol $|\ |$ are consistent with the notion of order of a set.

**Proposition 2.** If $H = \langle x \rangle$, then $|H| = |x|$ (where if one side of this equality is infinite, so is the other). More specifically

**(1)** if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of $H$, and

**(2)** if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.

*Proof:* Let $|x| = n$ and first consider the case when $n < \infty$. The elements $1, x, x^2, \ldots, x^{n-1}$ are distinct because if $x^a = x^b$, with, say, $0 \leq a < b < n$, then $x^{b-a} = x^0 = 1$, contrary to $n$ being the smallest positive power of $x$ giving the identity. Thus $H$ has at least $n$ elements and it remains to show that these are all of them. As we did in Example 1, if $x^t$ is any power of $x$, use the Division Algorithm to write $t = nq + k$, where $0 \leq k < n$, so

$$x^t = x^{nq+k} = (x^n)^q x^k = 1^q x^k = x^k \in \{1, x, x^2, \ldots, x^{n-1}\},$$

as desired.

Next suppose $|x| = \infty$ so no positive power of $x$ is the identity. If $x^a = x^b$, for some $a$ and $b$ with, say, $a < b$, then $x^{b-a} = 1$, a contradiction. Distinct powers of $x$ are distinct elements of $H$ so $|H| = \infty$. This completes the proof of the proposition.

Note that the proof of the proposition gives the method for reducing arbitrary powers of a generator in a finite cyclic group to the "least residue" powers. It is not a coincidence that the calculations of distinct powers of a generator of a cyclic group of order $n$ are carried out via arithmetic in $\mathbb{Z}/n\mathbb{Z}$. Theorem 4 following proves that these two groups are isomorphic.

First we need an easy proposition.

**Proposition 3.** Let $G$ be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides $m$.

*Proof:* By the Euclidean Algorithm (see Section 0.2 (6)) there exist integers $r$ and $s$ such that $d = mr + ns$, where $d$ is the g.c.d. of $m$ and $n$. Thus

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1.$$

This proves the first assertion.

If $x^m = 1$, let $n = |x|$. If $m = 0$, certainly $n \mid m$, so we may assume $m \neq 0$. Since some nonzero power of $x$ is the identity, $n < \infty$. Let $d = (m, n)$ so by the preceding result $x^d = 1$. Since $0 < d \leq n$ and $n$ is the smallest positive power of $x$ which gives the identity, we must have $d = n$, that is, $n \mid m$, as asserted.