(b) prove that $(1, 1)$ is the identity of $A \times B$, and
(c) prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

30. Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

31. Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.]

32. If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

33. Let x be an element of finite order n in G.
(a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n - 1$.
(b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

34. If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$ are all distinct.

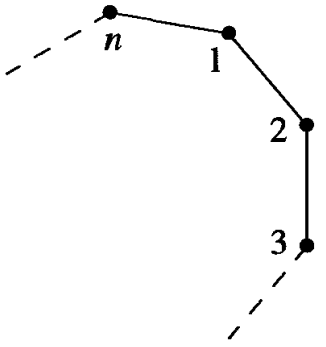
35. If x is an element of finite order n in G, use the Division Algorithm to show that *any* integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup (cf. Exercise 27 above) of G generated by x).

36. Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Exercise 32, every element has order ≤ 3). Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

1.2 DIHEDRAL GROUPS

An important family of examples of groups is the class of groups whose elements are symmetries of geometric objects. The simplest subclass is when the geometric objects are regular planar figures.

For each $n \in \mathbb{Z}^+$, $n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it. More precisely, we can describe the symmetries by first choosing a labelling of the n vertices, for example as shown in the following figure.

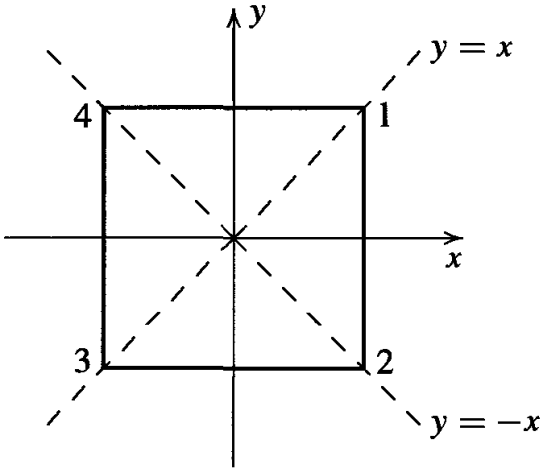


Then each symmetry s can be described uniquely by the corresponding permutation σ of $\{1, 2, 3, \ldots, n\}$ where if the symmetry s puts vertex i in the place where vertex j was originally, then σ is the permutation sending i to j. For instance, if s is a rotation of $2\pi/n$ radians clockwise about the center of the n-gon, then σ is the permutation sending i to $i + 1$, $1 \leq i \leq n - 1$, and $\sigma(n) = 1$. Now make D_{2n} into a group by defining st for $s, t \in D_{2n}$ to be the symmetry obtained by first applying t then s to the n-gon (note that we are viewing symmetries as functions on the n-gon, so st is just function composition — read as usual from right to left). If s, t effect the permutations σ, τ, respectively on the vertices, then st effects $\sigma \circ \tau$. The binary operation on D_{2n} is associative since composition of functions is associative. The identity of D_{2n} is the identity symmetry (which leaves all vertices fixed), denoted by 1, and the inverse of $s \in D_{2n}$ is the symmetry which reverses all rigid motions of s (so if s effects permutation σ on the vertices, s^{-1} effects σ^{-1}). In the next paragraph we show

$$|D_{2n}| = 2n$$

and so D_{2n} is called the *dihedral group of order* $2n$. In some texts this group is written D_n; however, D_{2n} (where the subscript gives the order of the group rather than the number of vertices) is more common in the group theory literature.

To find the order $|D_{2n}|$ observe that given any vertex i, there is a symmetry which sends vertex 1 into position i. Since vertex 2 is adjacent to vertex 1, vertex 2 must end up in position $i + 1$ or $i - 1$ (where $n + 1$ is 1 and $1 - 1$ is n, i.e., the integers labelling the vertices are read mod n). Moreover, by following the first symmetry by a reflection about the line through vertex i and the center of the n-gon one sees that vertex 2 can be sent to either position $i + 1$ or $i - 1$ by some symmetry. Thus there are $n \cdot 2$ positions the ordered pair of vertices 1, 2 may be sent to upon applying symmetries. Since symmetries are rigid motions one sees that once the position of the ordered pair of vertices 1, 2 has been specified, the action of the symmetry on all remaining vertices is completely determined. Thus there are exactly $2n$ symmetries of a regular n-gon. We can, moreover, explicitly exhibit $2n$ symmetries. These symmetries are the n rotations about the center through $2\pi i/n$ radian, $0 \leq i \leq n-1$, and the n reflections through the n lines of symmetry (if n is odd, each symmetry line passes through a vertex and the mid-point of the opposite side; if n is even, there are $n/2$ lines of symmetry which pass through 2 opposite vertices and $n/2$ which perpendicularly bisect two opposite sides). For example, if $n = 4$ and we draw a square at the origin in an x, y plane, the lines of symmetry are



the lines $x = 0$ (y-axis), $y = 0$ (x-axis), $y = x$ and $y = -x$ (note that "reflection" through the origin is not a reflection but a rotation of π radians).

Since dihedral groups will be used extensively as an example throughout the text we fix some notation and mention some calculations which will simplify future computations and assist in viewing D_{2n} as an abstract group (rather than having to return to the geometric setting at every instance). Fix a regular n-gon centered at the origin in an x, y plane and label the vertices consecutively from 1 to n in a clockwise manner. Let r be the rotation clockwise about the origin through $2\pi/n$ radian. Let s be the reflection about the line of symmetry through vertex 1 and the origin (we use the same letters for each n, but the context will always make n clear). We leave the details of the following calculations as an exercise (for the most part we shall be working with D_6 and D_8, so the reader may wish to try these exercises for $n = 3$ and $n = 4$ first):

(1) $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.
(2) $|s| = 2$.
(3) $s \neq r^i$ for any i.
(4) $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$, so

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

i.e., each element can be written *uniquely* in the form $s^k r^i$ for some $k = 0$ or 1 and $0 \leq i \leq n-1$.

(5) $rs = sr^{-1}$. [First work out what permutation s effects on $\{1, 2, \ldots, n\}$ and then work out separately what each side in this equation does to vertices 1 and 2.] This shows in particular that r and s do not commute so that D_{2n} is non-abelian.

(6) $r^i s = sr^{-i}$, for all $0 \leq i \leq n$. [Proceed by induction on i and use the fact that $r^{i+1}s = r(r^i s)$ together with the preceding calculation.] This indicates how to commute s with powers of r.

Having done these calculations, we now observe that the complete multiplication table of D_{2n} can be written in terms r and s alone, that is, all the elements of D_{2n} have a (unique) representation in the form $s^k r^i$, $k = 0$ or 1 and $0 \leq i \leq n-1$, and any product of two elements in this form can be reduced to another in the same form using only "relations" (1), (2) and (6) (reducing all exponents mod n). For example, if $n = 12$,

$$(sr^9)(sr^6) = s(r^9 s)r^6 = s(sr^{-9})r^6 = s^2 r^{-9+6} = r^{-3} = r^9.$$

Generators and Relations

The use of the generators r and s for the dihedral group provides a simple and succinct way of computing in D_{2n}. We can similarly introduce the notions of generators and relations for arbitrary groups. It is useful to have these concepts early (before their formal justification) since they provide simple ways of describing and computing in many groups. Generators will be discussed in greater detail in Section 2.4, and both concepts will be treated rigorously in Section 6.3 when we introduce the notion of free groups.

A subset S of elements of a group G with the property that every element of G can be written as a (finite) product of elements of S and their inverses is called a set of *generators* of G. We shall indicate this notationally by writing $G = \langle S \rangle$ and say G *is generated by* S or S *generates* G. For example, the integer 1 is a generator for the additive group $\mathbb{Z}$ of integers since every integer is a sum of a finite number of $+1$'s and -1's, so $\mathbb{Z} = \langle 1 \rangle$. By property (4) of D_{2n} the set $S = \{r, s\}$ is a set of generators of D_{2n}, so $D_{2n} = \langle r, s \rangle$. We shall see later that in a finite group G the set S generates G if every element of G is a finite product of elements of S (i.e., it is not necessary to include the inverses of the elements of S as well).

Any equations in a general group G that the generators satisfy are called *relations* in G. Thus in D_{2n} we have relations: $r^n = 1$, $s^2 = 1$ and $rs = sr^{-1}$. Moreover, in D_{2n} these three relations have the additional property that *any* other relation between elements of the group may be derived from these three (this is not immediately obvious; it follows from the fact that we can determine exactly when two group elements are equal by using only these three relations).

In general, if some group G is generated by a subset S and there is some collection of relations, say $R_1, R_2, \ldots, R_m$ (here each R_i is an equation in the elements from $S \cup \{1\}$) such that any relation among the elements of S can be deduced from these, we shall call these generators and relations a *presentation* of G and write

$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle.$$

One presentation for the dihedral group D_{2n} (using the generators and relations above) is then

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle. \tag{1.1}$$

We shall see that using this presentation to describe D_{2n} (rather than always reverting to the original geometric description) will greatly simplify working with these groups.

Presentations give an easy way of describing many groups, but there are a number of subtleties that need to be considered. One of these is that in an arbitrary presentation it may be difficult (or even impossible) to tell when two elements of the group (expressed in terms of the given generators) are equal. As a result it may not be evident what the order of the presented group is, or even whether the group is finite or infinite! For example, one can show that $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \rangle$ is a presentation of a group of order 4, whereas $\langle x_2, y_2 \mid x_2^3 = y_2^3 = (x_2 y_2)^3 = 1 \rangle$ is a presentation of an infinite group (cf. the exercises).

Another subtlety is that even in quite simple presentations, some "collapsing" may occur because the relations are intertwined in some unobvious way, i.e., there may be "hidden," or implicit, relations that are not explicitly given in the presentation but rather are consequences of the specified ones. This collapsing makes it difficult in general to determine even a lower bound for the size of the group being presented. For example, suppose one mimicked the presentation of D_{2n} in an attempt to create another group by defining:

$$X_{2n} = \langle x, y \mid x^n = y^2 = 1,\ xy = yx^2 \rangle. \tag{1.2}$$

The "commutation" relation $xy = yx^2$ determines how to commute y and x (i.e., how to "move" y from the right of x to the left), so that just as in the group D_{2n} every element in this group can be written in the form $y^k x^i$ with all the powers of y on the left and all

the powers of x on the right. Also, by the first two relations any powers of x and y can be reduced so that i lies between 0 and $n-1$ and k is 0 or 1. One might therefore suppose that X_{2n} is again a group of order $2n$. This is not the case because in this group there is a "hidden" relation obtained from the relation $x = xy^2$ (since $y^2 = 1$) by applying the commutation relation and the associative law repeatedly to move the y's to the left:

$$\begin{aligned} x = xy^2 = (xy)y = (yx^2)y = (yx)(xy) = (yx)(yx^2) \\ = y(xy)x^2 = y(yx^2)x^2 = y^2x^4 = x^4. \end{aligned}$$

Since $x^4 = x$ it follows by the cancellation laws that $x^3 = 1$ in X_{2n}, and from the discussion above it follows that X_{2n} has order at most 6 for any n. Even more collapsing may occur, depending on the value of n (see the exercises).

As another example, consider the presentation

$$Y = \langle u, v \mid u^4 = v^3 = 1,\ uv = v^2u^2 \rangle. \tag{1.3}$$

In this case it is tempting to guess that Y is a group of order 12, but again there are additional implicit relations. In fact this group Y degenerates to the trivial group of order 1, i.e., u and v satisfy the additional relations $u = 1$ and $v = 1$ (a proof is outlined in the exercises).

This kind of collapsing does not occur for the presentation of D_{2n} because we showed by independent (geometric) means that there *is* a group of order $2n$ with generators r and s and satisfying the relations in (1). As a result, a group with only these relations must have order at *least* $2n$. On the other hand, it is easy to see (using the same sort of argument for X_{2n} above and the commutation relation $rs = sr^{-1}$) that any group defined by the generators and relations in (1) has order at *most* $2n$. It follows that the group with presentation (1) has order exactly $2n$ and also that this group is indeed the group of symmetries of the regular n–gon.

The additional information we have for the presentation (1) is the existence of a group of known order satisfying this information. In contrast, we have no independent knowledge about any groups satisfying the relations in either (2) or (3). Without such independent "lower bound" information we might not even be able to determine whether a given presentation just describes the trivial group, as in (3).

While in general it is necessary to be extremely careful in prescribing groups by presentations, the use of presentations for known groups is a powerful conceptual and computational tool. Additional results about presentations, including more elaborate examples, appear in Section 6.3.

EXERCISES

In these exercises, D_{2n} has the usual presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$.

1. Compute the order of each of the elements in the following groups:
   (a) D_6 **(b)** D_8 **(c)** D_{10}.
2. Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.
3. Use the generators and relations above to show that every element of D_{2n} which is not a