

## §14 Dihedral Groups

In this paragraph, we examine the symmetry groups of regular polygons.

Let  $F$  be any nonempty subset of the Euclidean plane  $E$ . Here  $F$  might be a set with a single point, a line, a geometric figure or an arbitrary subset of  $E$ . Let  $\alpha \in S_E$ . We put

$$F\alpha = \{x\alpha : x \in F\} = \{y \in E : y = x\alpha \text{ for some } x \in F\}.$$

$F\alpha$  is called the *image of  $F$  under  $\alpha$* . Clearly,

$$F1 = \{x1 : x \in F\} = \{x : x \in F\} = F$$

and we have

$$\begin{aligned} F(\alpha\beta) &= \{x(\alpha\beta) : x \in F\} = \{(x\alpha)\beta : x \in F\} \\ &= \{(x\alpha)\beta : x\alpha \in F\alpha\} = \{y\beta : y \in F\alpha\} = (F\alpha)\beta \end{aligned}$$

for all  $\alpha, \beta \in S_E$ . We record this as a lemma.

**14.1 Lemma:** *Let  $F$  be a nonempty subset of  $E$  and let  $\alpha, \beta \in S_E$ . Then*

$$F1 = F$$

and

$$F(\alpha\beta) = (F\alpha)\beta. \quad \square$$

Let  $P$  be a point in  $E$  and  $\alpha \in S_E$ . We say  $\alpha$  *fixes*  $P$  if  $P\alpha = P$ . We also say  $P$  is a *fixed point of  $\alpha$*  in this case. Let  $\emptyset \neq F \subseteq E$ . We say  $\alpha$  *fixes*  $F$  (as a set) if  $F\alpha = F$ . This means of course  $F\alpha \subseteq F$  and  $F \subseteq F\alpha$ , so  $P\alpha \in F$  for all  $P \in F$  and also, for every  $Q \in F$ , there is a  $P \in F$  such that  $Q = P\alpha$ . The reader should not confuse this with  $\alpha$  fixing  $F$  pointwise. We say that  $\alpha$  *fixes  $F$  pointwise* if  $P\alpha = P$  for all  $P \in F$ , i.e., if  $\alpha$  fixes every point of  $F$ . As an example, let  $A$  be the  $x$ -axis  $\{(x,0) : x \in \mathbb{R}\}$ . The translation  $\tau_{1,0}$  fixes  $A$  as a set, but not pointwise. On the other hand, the reflection  $\sigma : (x,y) \rightarrow (x,-y)$  in the  $x$ -axis fixes  $A$  pointwise.

This terminology is meaningful for all elements of  $S_E$ , but we consider only isometries in this paragraph.

**14.2 Definition:** Let  $F$  be a nonempty subset of  $E$  and let  $\alpha \in \text{Isom } E$ . If  $F\alpha = F$ , then  $\alpha$  is called a *symmetry of  $F$* .

So a symmetry of  $F$  is an isometry that fixes  $F$  as a set. A symmetry of  $F$  is *not* a property of  $F$ . It is a mapping.

**14.3 Examples:** (a) Let  $F = \{(0,0)\}$  be the subset of  $E$  consisting of the origin only. Any rotation  $\rho_\varphi$  about the origin is a symmetry of  $F$ , since any rotation about the origin is an isometry and fixes the origin (or, equivalently, fixes  $F$ ).

(b) Let  $F = \{(x,y) \in E: y = mx\}$  be the line whose cartesian equation is  $y = mx$  (where  $m \in \mathbb{R}$ ). Then the translation  $\tau_{1,m}$  is a symmetry of  $F$  since

$$\begin{aligned} F\tau_{1,m} &= \{f\tau_{1,m} \in E: f \in F\} \\ &= \{(x,y)\tau_{1,m} \in E: y = mx\} \\ &= \{(x+1,y+m) \in E: y = mx\} \\ &= \{(x+1,(x+1)m) \in E: x \in \mathbb{R}\} \\ &= \{(u,v) \in E: v = mu\} \\ &= F. \end{aligned}$$

Similarly, all translations of the form  $\tau_{a,am}$  is a symmetry of  $F$ . We note that such translations form a group. In fact, the symmetries of any nonempty subset of  $E$  form a group.

**14.4 Theorem:** Let  $F$  be a nonempty subset of the Euclidean plane  $E$  and let  $\text{Sym } F$  be the set of all symmetries of  $F$ , so that

$$\text{Sym } F := \{\alpha \in \text{Isom } E: F\alpha = F\}.$$

Then  $\text{Sym } F$  is a subgroup of  $\text{Isom } E$ .

**Proof:** We have  $F\iota = F$  by Lemma 14.1, so  $\iota \in \text{Sym } F$  and  $\text{Sym } F$  is not empty. Now we use Lemma 9.2.

(i) If  $\alpha, \beta \in \text{Sym } F$ , then  $F\alpha = F$  and  $F\beta = F$ , so  $F(\alpha\beta) = (F\alpha)\beta = F\beta = F$  by Lemma 14.1. Thus  $\alpha\beta \in \text{Sym } F$ .

(ii) If  $\alpha \in \text{Sym } F$ , then  $F\alpha = F$ , so  $F(\alpha^{-1}) = (F\alpha)\alpha^{-1} = F(\alpha\alpha^{-1}) = F I = F$  by Lemma 14.1. Thus  $\alpha^{-1} \in \text{Sym } F$ .

It follows that  $\text{Sym } F \leq \text{Isom } E$ . □

**14.5 Definition:** Let  $F$  be a nonempty subset of  $E$ . Then

$$\text{Sym } F = \{ \alpha \in \text{Isom } E : F\alpha = F \}$$

is called the *symmetry group of  $F$* .

We now study the symmetry groups of regular polygons. For our purposes, it will be convenient to define regular polygons as follows. Let  $K$  be a circle and let  $P_1, P_2, \dots, P_n$  be  $n$  points on this circle  $K$  such that each one of the arcs  $\widehat{P_1 P_2}, \widehat{P_2 P_3}, \dots, \widehat{P_{n-1} P_n}$  subtends an angle of  $2\pi/n$  radians at the center of  $K$  (where  $n \geq 3$ ). So the points  $P_1, P_2, \dots, P_n$  divide the circle  $K$  into  $n$  circular arcs of equal length. The union of the line segments  $\overline{P_1 P_2}, \overline{P_2 P_3}, \dots, \overline{P_{n-1} P_n}, \overline{P_n P_1}$  is called a *regular  $n$ -gon*. The circle  $K$  is called *the circumscribing circle* of this regular  $n$ -gon. This is justified since a regular  $n$ -gon has a unique circumscribing circle. The center of the circumscribing circle is called the *center* of the regular  $n$ -gon and the points  $P_1, P_2, \dots, P_n$  are called the *vertices* of the regular  $n$ -gon.

Let  $F$  be a regular  $n$ -gon. We want to determine  $\text{Sym } F$ . It is geometrically evident that any  $\alpha$  in  $\text{Sym } F$  maps a vertex to a vertex and fixes the center of  $F$ . We use this fact without proof. A proof is outlined in the exercises at the end of this paragraph. Let  $P_1, P_2, \dots, P_n$  be the vertices and let  $C$  be the center of  $F$ . We assume the notation so chosen that  $P_1, P_2, \dots, P_n$  are consecutive vertices as we trace the regular  $n$ -gon counterclockwise. In the following discussion,  $P_{n+1}$  will stand for  $P_1$ ,  $P_{n+2}$  for  $P_2$ , in general  $P_{n+k}$  for  $P_k$ . In other words, the indices will be read modulo  $n$ .

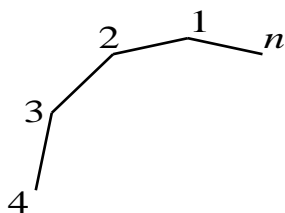


Figure 1

Now let  $\alpha \in \text{Sym } F$ . Then  $\alpha$  is completely determined by its effect on three distinct points not on a straight line (Lemma 13.17). For example,  $\alpha$  is determined by  $C\alpha, P_1\alpha, P_2\alpha$ . We have already remarked that  $C\alpha = C$ . Also  $P_1\alpha = P_k$  for some  $k \in \{1, 2, \dots, n\}$ . What about  $P_2$ ? Since  $\alpha$  is an isometry,  $P_2\alpha$  will be a vertex whose distance from  $P_k$  is equal to the distance between  $P_1$  and  $P_2$ . Thus  $P_2\alpha$  will be adjacent to  $P_k$ : it is either  $P_{k-1}$  or  $P_{k+1}$ . We see that there are  $n$  choices for  $P_1\alpha$  and, once the choice for  $P_1\alpha$  has been made, there are two choices for  $P_2\alpha$ . Hence there are at most  $n \cdot 2 = 2n$  isometries in  $\text{Sym } F$ . We exhibit  $2n$  symmetries of  $F$  and this will prove  $|\text{Sym } F| = 2n$ .

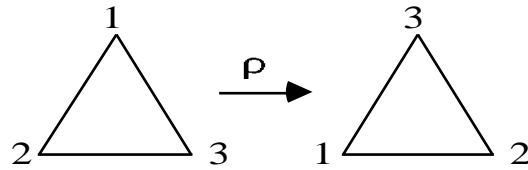


Figure 2

First we examine the special case  $n = 3$ , when  $F$  is an equilateral triangle. Consider a rotation about the center of  $F$  through an angle of  $2\pi/3$  radians, which we denote by  $\rho$ . Under  $\rho$ , the vertices  $P_1, P_2, P_3$  take the places of  $P_2, P_3, P_4 = P_1$  respectively. It is seen from Figure 3 that  $\rho^2$  maps  $P_1, P_2, P_3$  respectively to  $P_3, P_2, P_1$  and that  $\rho^3$  fixes  $P_1, P_2, P_3$ , which implies  $\rho^3 = \iota$ . We found three symmetries of  $F$ , namely  $\iota, \rho, \rho^2$ . Since  $\rho^3 = \iota \neq \rho$ , we see that  $\langle \rho \rangle$  is a cyclic subgroup of order 3 of  $\text{Sym } F$ .

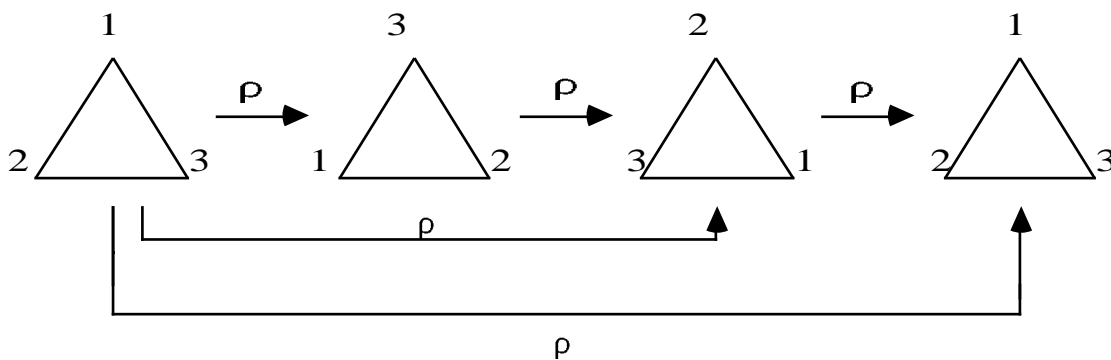


Figure 3

Now consider the reflection in the perpendicular bisector of  $\overline{P_2P_3}$ , which passes through  $P_1$ . We designate this reflection as  $\sigma$ . Under  $\sigma$ , the vertex

$P_1$  remains fixed and the vertices  $P_2$  and  $P_3$  exchange their places. We know  $\sigma^2 = \iota$  (Lemma 13.13). From Figure 4, we read off  $\sigma\rho^{-1} = \sigma\rho^2 = \rho\sigma$ . Using  $\rho$  and  $\sigma$ , we obtain two new symmetries of  $F$ , namely  $\rho\sigma$  and  $\rho^2\sigma$ . The reader may check that  $\rho\sigma$  is the reflection in the perpendicular bisector of  $\overline{P_1P_3}$  and that  $\rho^2\sigma$  is the reflection in the perpendicular bisector of  $\overline{P_1P_2}$ . From the geometric meaning of these mappings, or from their effect on  $P_1, P_2, P_3$ , we infer that  $\iota, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma$  are distinct. Thus they form the symmetry group of  $F$ :  $\text{Sym } F = \{\iota, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$ . In particular,  $|\text{Sym } F|$  is equal to 6.

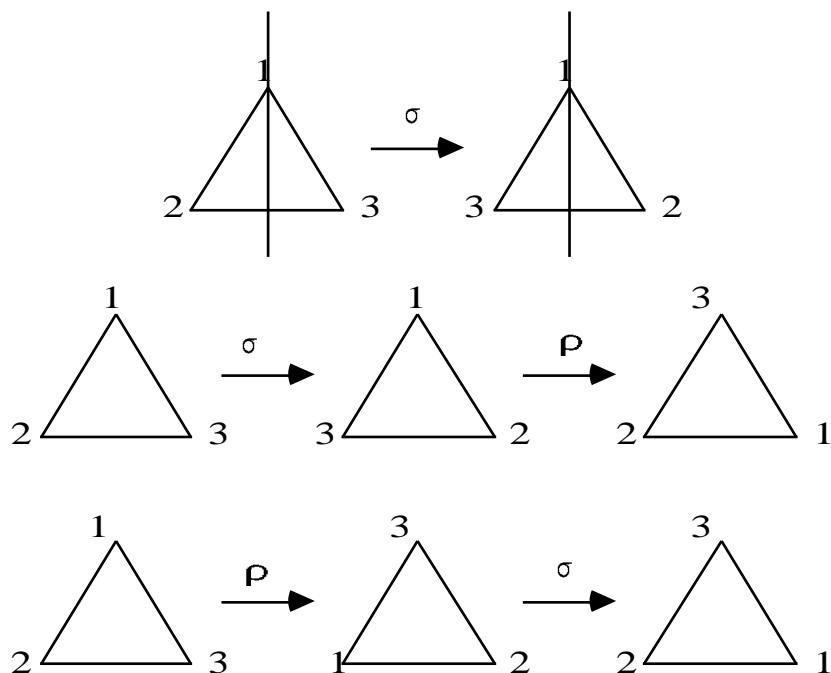


Figure 4

The discussion of a general regular polygon follows much the same lines. Consider a rotation about the center of  $F$  through an angle of  $2\pi/n$  radians, which we denote by  $\rho$ . Under  $\rho$ , the vertices  $P_1, P_2, \dots, P_n$  are mapped respectively to  $P_2, P_3, \dots, P_n, P_1$ . It is seen that  $\rho^k$  maps  $P_1, P_2, \dots, P_n$  respectively to  $P_{k+1}, P_{k+2}, \dots, P_{k+n}$ , where  $k$  is any integer. Thus  $\rho^k = \iota$  if and only if  $P_{k+i} = P_i$  that is, if and only if  $k+i \equiv i \pmod{n}$  for all  $i$ , so if and only if  $n|k$ , from which we obtain  $o(\rho) = n$ . In this way, we found  $n$  symmetries of  $F$ , namely  $\iota, \rho, \rho^2, \dots, \rho^n$ . Here  $\langle \rho \rangle$  is a cyclic subgroup of order  $n$  of  $\text{Sym } F$ .

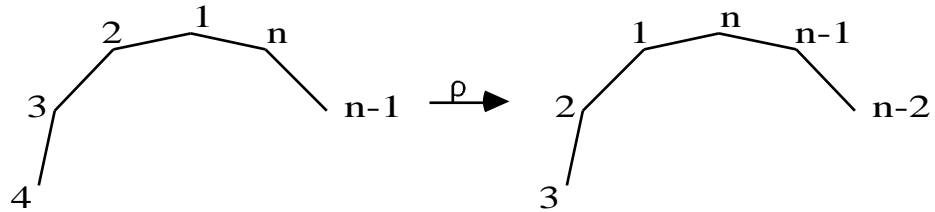


Figure 5

Now consider the reflection  $\sigma$  in the angular bisector of the angle  $\angle P_n P_1 P_2$ . The bisector of this angle passes through  $P_{(n/2)+1}$  if  $n$  is even and through the midpoint of  $P_{(n+1)/2} P_{(n+3)/2}$  if  $n$  is odd. One reads off from Figure 6 that  $P_k \sigma = P_{n+2-k}$  for  $k = 1, 2, \dots, n$ .

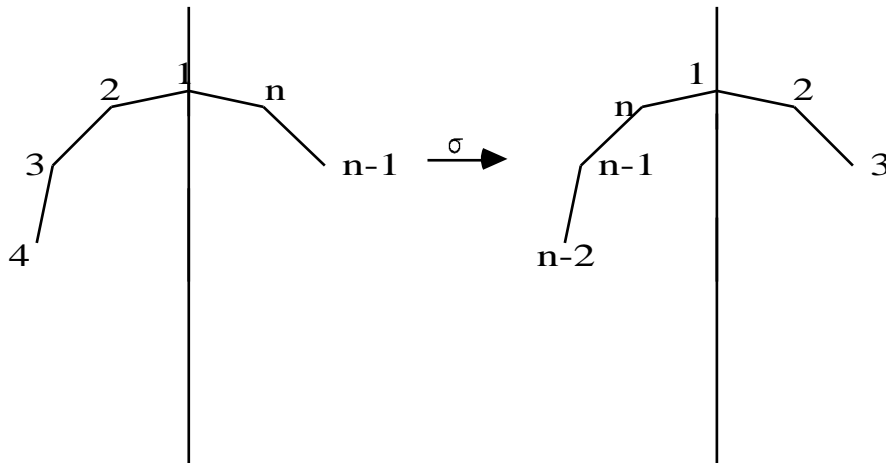


Figure 6

Thus we have, for any  $j = 1, 2, \dots, n$ ,

$$P_j \sigma \rho = P_{n+2-j} \rho = P_{(n+2-j)+1} = P_{n-j+3},$$

$$P_j \rho^{-1} \sigma = P_{j-1} \sigma = P_{(n+2)-(j-1)} = P_{n-j+3},$$

so  $\sigma \rho = \rho^{-1} \sigma$ , as can be seen from Figure 7 too.

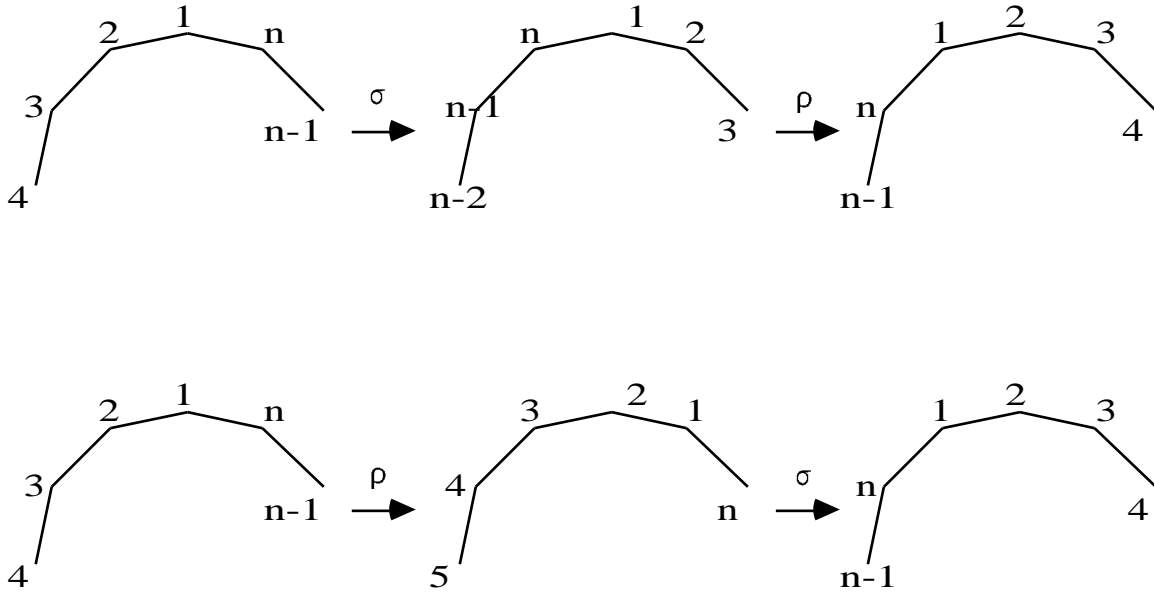


Figure 7

Using  $\rho$  and  $\sigma$ , we obtain  $n - 1$  new symmetries  $\rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma$  of  $F$ . These are reflections in certain lines. The reader may verify this assertion in the case of squares, regular pentagons, regular hexagons and regular heptagons. In particular, we have  $(\rho^m\sigma)^2 = \iota$  for any  $m = 0, 1, \dots, n - 1$ . This follows also from the lemma below.

**14.6 Lemma:** *Let  $G$  be a group and let  $\rho, \sigma \in G$  be such that  $\sigma^2 = 1$  and  $\sigma\rho = \rho^{-1}\sigma$ . Then  $\sigma\rho^n = \rho^{-n}\sigma$  for all  $n \in \mathbb{Z}$ .*

**Proof:** The claim is certainly true when  $n = 0$ , and also when  $n = 1$  by hypothesis. We prove  $\sigma\rho^n = \rho^{-n}\sigma$  for all  $n \in \mathbb{N}$  by induction on  $n$ . Suppose we proved it for  $n = k \in \mathbb{N}$ , so that  $\sigma\rho^k = \rho^{-k}\sigma$ , then it is true for  $n = k + 1$ , since  $\sigma\rho^{k+1} = \sigma(\rho^k\rho) = (\sigma\rho^k)\rho = (\rho^{-k}\sigma)\rho = \rho^{-k}(\sigma\rho) = \rho^{-k}(\rho^{-1}\sigma) = (\rho^{-k}\rho^{-1})\sigma = \rho^{-(k+1)}\sigma$ . This shows  $\sigma\rho^n = \rho^{-n}\sigma$  for all  $n \geq 0$ . We must further show this when  $n < 0$ , or, equivalently, that  $\sigma\rho^n = \rho^n\sigma$  for all  $n \in \mathbb{N}$ . This will follow from what we proved above, with  $\rho^{-1}, \sigma$  in place of  $\rho, \sigma$ . Observe that  $\sigma^2 = 1, \sigma\rho = \rho^{-1}\sigma$  implies

$$\begin{aligned} \sigma\sigma\rho &= \sigma\rho^{-1}\sigma \\ \rho &= \sigma\rho^{-1}\sigma \\ \rho\sigma &= \sigma\rho^{-1}\sigma\sigma \\ \rho\sigma &= \sigma\rho^{-1} \end{aligned}$$

and, taking inverses,  $\sigma\rho^{-1} = (\rho^{-1})^{-1}\sigma,$

so the hypothesis is valid with  $\rho^{-1}, \sigma$  in place of  $\rho, \sigma$ . Then we get

$$\sigma(\rho^{-1})^n = (\rho^{-1})^n \sigma \quad \text{for all } n \in \mathbb{N},$$

and thus  $\sigma \rho^n = \rho^n \sigma$  for all  $n \in \mathbb{N}$ . This completes the proof.  $\square$

We found  $2n$  symmetries of  $F$ :  $\iota, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma$ . These are distinct (why?) From  $|\text{Sym } F| \leq 2n$ , we get  $|\text{Sym } F| = 2n$  and

$$\text{Sym } F = \{\iota, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma\}.$$

Every element in  $\text{Sym } F$  can be written as a product of a suitable power of  $\rho$  by suitable power of  $\sigma$ , which remark we summarize by saying that  $\rho$  and  $\sigma$  generate  $\text{Sym } F$ . We also say  $\text{Sym } F$  is generated by  $\rho$  and  $\sigma$ , and that  $\rho$  and  $\sigma$  are generators of  $\text{Sym } F$ . The notation  $\langle \rho, \sigma \rangle$  denotes a group with two generators. Including the relations  $\rho^n = \iota$ ,  $\sigma^2 = \iota$  and  $\sigma\rho = \rho^{-1}\sigma$ , we write

$$\text{Sym } F = \langle \rho, \sigma : \rho^n = \iota, \sigma^2 = \iota, \sigma\rho = \rho^{-1}\sigma \rangle.$$

**14.7 Definition:** Let  $G$  be a group having elements  $a, b$  such that

$$o(a) = n, o(b) = 2, ba = a^{-1}b,$$

$$G = \{a^k b^r : k = 0, 1, \dots, n-1, r = 0, 1\},$$

where  $n \geq 2$ . Then  $G$  is called a *dihedral group of order  $2n$* .

It is easily seen from  $o(a) = n$  and  $o(b) = 2$  that the elements of  $G$  displayed in Definition 14.7 are indeed distinct. Using Lemma 14.6, products in  $G$  can be brought to the form  $a^k b^r$ . Hence  $G$  is really of order  $n$ . In a dihedral group of order 8, for example, we have

$$a^2 b a b^3 a^5 a^7 b^{-1} = a^2 b a b a^{12} b = a^2 . b a b . a^4 b = a^2 . a^{-1} . a^4 b = a^5 b$$

with the foregoing notation. (The exponent of  $a$  changes sign when  $b$  "passes through"  $a$  to the other side.)

We see that symmetry groups of regular polygons are dihedral groups. We write  $D_{2n}$  for a dihedral group of order  $2n$ . (Warning: some authors write  $D_n$  for a dihedral group of order  $2n$ .) Henceforward, we write  $D_{2n}$  instead of  $\text{Sym } F$  ( $F$  being a regular polygon with  $n$  sides). The ambiguity

in " $D_{2n}$ " (whether it designates an arbitrary dihedral group or the particular dihedral group  $Sym F$ ) is harmless.

Some people use Definition 14.7 only when  $n \geq 3$ . They do not consider  $D_4$  as a dihedral group. This is consistent with the fact that  $D_4$  is not the symmetry group of any regular polygon (see however Ex.10). But then they have to formulate the following theorem of Leonardo da Vinci (yes, of Leonardo da Vinci (1452-1519)) less beautifully.

**14.8 Theorem:** *A finite subgroup of  $Isom E$  is either a cyclic group or a dihedral group.*

This theorem will not be used in the sequel and its proof is left to the reader.

## Exercises

1. Let  $\alpha$  be an isometry and  $F_1, F_2$  nonempty subsets of  $E$ . Show that  $(F_1 \cup F_2)\alpha = F_1\alpha \cup F_2\alpha$  and  $(F_1 \cap F_2)\alpha = F_1\alpha \cap F_2\alpha$ . Generalize to arbitrary unions and intersections.
2. Let  $\alpha$  be an isometry and  $P, Q$  two distinct points in  $E$ . Show that  $(\overline{PQ})\alpha = \overline{P\alpha Q\alpha}$  and  $(PQ)\alpha = P\alpha Q\alpha$ . (Hint:  $\overline{PQ} = \{R \in E: d(P,R) + d(R,Q) = d(P,Q)\}$ .)
3. Let  $\alpha$  be an isometry and  $R$  the midpoint of  $\overline{PQ}$ . Show that  $R\alpha$  is the midpoint of  $\overline{P\alpha Q\alpha}$ .
4. Let  $\alpha$  be an isometry and  $\triangle PQR$  a triangle (i.e., the union of the segments  $\overline{PQ}, \overline{QR}, \overline{PR}$ ). Show that  $(\triangle PQR)\alpha = \triangle P\alpha Q\alpha R\alpha$ . (By the side-side-side condition, the triangles  $\triangle PQR$  and  $\triangle P\alpha Q\alpha R\alpha$  are congruent, hence  $\angle PQR$  and  $\angle P\alpha Q\alpha R\alpha$  are equal: isometries preserve angles. In particular, isometries preserve perpendicularity and so also parallelity.)

5. Let  $P_1, P_2, \dots, P_n$  be the vertices of a regular  $n$ -gon. If  $n$  happens to be odd, let  $Q_i$  be the midpoint of the side  $\overline{P_{[(n-1)/2+i]} P_{[(n+1)/2+i]}$  ( $i = 1, 2, \dots, n$ ). Prove that the center  $C$  of the regular  $n$ -gon is uniquely determined as the midpoint of  $\overline{P_i P_{i+(n/2)}}$  if  $n$  is even and as the midpoint of  $\overline{P_i Q_i}$  if  $n$  is odd. (As the radius of a circumscribing circle is equal to  $d(P_i, C)$ , this proves that a circumscribing circle is completely determined by the vertices. Hence there is a unique circumscribing circle of a regular  $n$ -gon.)

6. Let  $\alpha$  be an isometry and  $M$  a regular  $n$ -gon. Let  $C$  be the center of the regular  $n$ -gon. Prove the following assertions.

(a)  $M\alpha$  is a regular  $n$ -gon with center  $C\alpha$ .

(b) If  $\alpha$  is a symmetry of  $M$ , then  $C\alpha = C$ .

(c) If  $\alpha$  is a symmetry of  $M$ , then  $\{P_1, P_2, \dots, P_n\}\alpha = \{P_1, P_2, \dots, P_n\}$ .

(Under a symmetry of  $M$ , a vertex is mapped to a vertex. Hint: A point  $P$  on  $M$  is a vertex if and only if  $d(P, C) = \text{radius of the circumscribing circle}$ .)

7. Let  $m$  be a real number. Prove that  $\{\tau_{a, am} : \alpha \in \mathbb{R}\}$  is a subgroup of  $Isom E$  without appealing to Theorem 14.4.

8. Let  $P$  be a point and  $m$  a line. Find all isometries that fix  $P$ , all isometries that fix  $m$  and all isometries that fix  $m$  pointwise. Show directly that these three sets are subgroup of  $Isom E$ .

9. Let  $F$  be a nonempty subset of  $E$ . Is  $\{\alpha \in Isom E : F\alpha \subseteq F\}$  necessarily a subgroup of  $Isom E$ ?

10. Find the symmetry group of a rectangle that is not a square.

11. With the notation of Definition 14.7, what is  $|D_{2n}; \langle a \rangle|$ ?

12. Prove Theorem 14.8.

13. Let  $\tau: \mathbb{R} \rightarrow \mathbb{R}$ ,  $\sigma: \mathbb{R} \rightarrow \mathbb{R}$ . Prove the following assertions.

$$x \rightarrow x + 1 \quad x \rightarrow -x$$

(a)  $\tau, \sigma \in S_{\mathbb{R}}$ .

(b)  $|x - y| = |x\tau - y\tau| = |x\sigma - y\sigma|$ . (So  $\tau$  and  $\sigma$  preserve distance in  $\mathbb{R}$ .)

For this reason, they are said to be *isometries of  $\mathbb{R}$* .)

(c)  $o(\tau) = \infty$  and  $o(\sigma) = 2$ .

(d)  $\sigma\tau = \tau^{-1}\sigma$ . (Thus  $\tau, \sigma$  satisfy the conditions on  $a, b$  in Definition 14.7, except  $n$  is replaced by  $\infty$  here. A *dihedral group of infinite order* is a group  $D_\infty$  having element  $a, b$  such that  $o(a) = \infty$ ,  $o(b) = 2$ ,  $ba = a^{-1}b$  and

$$G = \{a^k b^r : k \in \mathbb{Z}, r = 0, 1\}.$$

The group generated by  $\tau, \sigma$  is an example of a dihedral group of infinite order.)

14. Prove that a group generated by two distinct elements  $a, b$  such that  $o(a) = 2 = o(b)$  is a dihedral group (of finite or infinite order).

15. Let  $n$  be any natural number or  $\infty$ . Find a group  $G$  and  $a, c \in G$  such that  $o(a) = 2 = o(c)$  and  $o(ac) = n$ . (So  $o(ac)$  cannot be determined from  $o(a)$  and  $o(c)$  alone.)