involve

a journal of mathematics

Maximal subgroups of the semigroup of partial symmetries of a regular polygon

Thomas L. Shelly and Janet E. Mills

mathematical sciences publishers

2008 Vol. 1, No. 1

INVOLVE 1:1(2008)

Maximal subgroups of the semigroup of partial symmetries of a regular polygon

Thomas L. Shelly and Janet E. Mills

(Communicated by Scott Chapman)

The semigroup of partial symmetries of a polygon P is the collection of all distance-preserving bijections between subpolygons of P, with composition as the operation. Around every idempotent of the semigroup there is a maximal subgroup that is the group of symmetries of a subpolygon of P. In this paper we construct all of the maximal subgroups that can occur for any regular polygon P, and determine for which P there exist nontrivial cyclic maximal subgroups, and for which there are only dihedral maximal subgroups.

1. Introduction and basic properties

The semigroup of partial symmetries of a polygon is a natural generalization of the group of symmetries of a polygon. In this paper we will assume knowledge of an undergraduate abstract algebra course and will generally use the terminology of Gallian [2002]. The group of symmetries of a polygon P is the set of distance-preserving mappings of P onto P, with composition as the operation. In particular, for any $n > 2$, the group of symmetries of a regular n-gon is a group, called the dihedral group, with $2n$ elements, and is denoted by D_n. The elements of this group are completely determined by the movement of the vertices, and D_n can be considered as a subgroup of the group of all permutations of the vertices of the polygon, under composition.

To generalize the notion of symmetries of a polygon, we first need to describe what a subpolygon should be. Let P be a convex polygon with set of vertices $V(P) = \{v_1, v_2, \ldots, v_n\}$, listed clockwise, where there exists an edge between v_i and v_{i+1} for $i = 1, 2, \ldots, n-1$, and an edge between v_n and v_1. Let

$$A = \{v_{i_1}, v_{i_2}, \ldots, v_{i_m}\}$$

be a subset of $V(P)$, where $i_1 < i_2 < \ldots < i_m$ and let P_A be the polygon with edges between v_{i_j} and $v_{i_{j+1}}$ for $j = 1, 2, \ldots, m-1$, and between v_{i_m} and v_{i_1}. The polygon

MSC2000: 20M18.
Keywords: semigroup, polygon, symmetries.

P_A is called a *subpolygon* of P, and in particular, P_A is said to be the subpolygon formed by A. Note that if v_{i_j} and $v_{i_{j+1}}$ are adjacent in P then the edge between them is still an edge in P_A; otherwise, the edge between them is new. Note also that the subpolygons include those with no vertices (the empty polygon), exactly one vertex (a point), or two vertices (a line segment).

For each subset of $V(P)$, there is a unique subpolygon described since the indices on the vertices must be increasing and each subpolygon is a convex polygon. The set of all subpolygons of P will be denoted by Π. Now we must describe the semigroup of partial symmetries of a convex polygon P. This class of semigroups was first defined in [Mills 1990b], and some of its properties explored in [Mills 1990a; 1993]. The domain and range of a function α will be denoted by $\operatorname{dom}\alpha$ and $\operatorname{ran}\alpha$ respectively.

Definition. Let P be a convex polygon. On the set

$$S = S(P) = \{\alpha : A \to B \mid P_A, P_B \in \Pi, \text{ and } \alpha \text{ is a distance-preserving bijection}\},$$

define composition by $x\alpha\beta = (x\alpha)\beta$ for all $x \in \operatorname{dom}\alpha$ such that $x\alpha \in \operatorname{dom}\beta$. Then under this operation, S is a semigroup, called the *semigroup of partial symmetries* of the polygon P.

Note that if α is in S and maps A onto B, then α^{-1} is also a distance-preserving bijection of B onto A, so α^{-1} is in S. The semigroup S is an example of an inverse semigroup. That is, for each $\alpha \in S$, there is a unique $\beta \in S$ such that $\alpha\beta\alpha = \alpha$ and $\beta\alpha\beta = \beta$. In our semigroup, for $\alpha \in S$, the mapping α^{-1} serves as the needed β.

An *idempotent* of S is any α such that $\alpha^2 = \alpha$. It is easy to see that because the mappings are one-to-one, α is an idempotent if and only if α is the identity on its domain A, denoted by ι_A. In any inverse semigroup the idempotents form a skeleton of the semigroup, and around every idempotent there is a maximal subgroup with that idempotent as its identity. In S, if A is a subset of $V(P)$, then the maximal subgroup with ι_A as its identity is

$$\begin{aligned} H_A &= \{\alpha \in S \mid \text{ there exists a } \beta \in S \text{ such that } \alpha\beta = \beta\alpha = \iota_A\} \\ &= \{\alpha \in S \mid \operatorname{dom}\alpha = \operatorname{ran}\alpha = A\}. \end{aligned}$$

This is the largest subgroup of S having ι_A as its identity.

It is the purpose of this paper to determine, for a regular polygon P, exactly which groups can occur as a maximal subgroup of $S(P)$. It is clear from the description above that the maximal subgroup around ι_A is the group of symmetries of the subpolygon P_A. Therefore, the effort to find all maximal subgroups of S reduces to describing the group of symmetries of each subpolygon of P. As is well known, the group of symmetries of any polygon is either a dihedral group or a cyclic group [Gallian 2002, Theorem 27.1]. The problem here is that we have a particular regular polygon P, and need to determine exactly which dihedral and cyclic groups can occur as symmetry groups of subpolygons of that polygon P.

From now on, we will assume that P is a regular polygon with n vertices. The semigroup $S(P)$ has an identity ι_P, and the maximal subgroup around ι_P is just the group of symmetries of P, or D_n. As we shall see, this subgroup plays an important part in determining the other maximal subgroups. Therefore, we need to recall some information about the group D_n. In particular, D_n is a group with $2n$ elements, having n reflections and n rotations. All reflections are about some line of symmetry of P that passes through the center of P. If n is even, every line of symmetry passes through two vertices or through the midpoint between two vertices, whereas if n is odd, every line of symmetry passes through exactly one vertex. Since P is regular, the rotations form a subgroup generated by ρ, which is a rotation about the center of P through $2\pi/n$ radians. This subgroup is often written as $\langle\rho\rangle$, the cyclic subgroup generated by ρ, which is isomorphic to $\mathbb{Z}_n$, the group of integers modulo n. In this paper, ρ will always denote this rotation.

2. Maximal subgroups

In this section we find all maximal subgroups of S for any regular polygon P. In addition, we provide a description of all subpolygons with rotational symmetry and we give a method for constructing subpolygons with cyclic symmetry groups. For the remainder of the paper we use the following notation: Greek letters are used to represent elements of S, and the letters v and w are used to represent vertices. Thus any expression of the form $\alpha\beta$ denotes composition, whereas the expression $v\alpha = w$ says that the vertex v is mapped to w under α (we always write the argument of the function to the left of the function, as in the definition of S in Section 1). The letter d is always used to represent an arbitrary element of D_n.

It was shown in [Mills 1993] that for a regular polygon P, every element $\alpha \in S$ can be extended to an element in the group of symmetries of P. That is, if $\operatorname{dom}\alpha = A$ then $\alpha = \iota_A d$ for some $d \in D_n$. Further, it was shown that if A has at least 3 elements, then d is unique. For the remainder of the paper, we always take any subset A of $V(P)$ to have more than two elements to ensure every element in the maximal subgroup H_A extends uniquely to D_n. Not much is lost by this restriction, since if $|A| \leq 2$ then P_A is either a point or a line segment, and H_A is either $\mathbb{Z}_1$ or $\mathbb{Z}_2$. This unique extension guarantees that rotations in H_A are extended to rotations in D_n and reflections in H_A are extended to reflections in D_n. More specifically, we can connect elements in H_A to those in D_n as follows.

Lemma 2.1. *Let α and β be elements of a maximal subgroup H_A, with $|A| > 2$, such that $\alpha = \iota_A d_1$ and $\beta = \iota_A d_2$ for $d_1, d_2 \in D_n$. Then the following are true*:

(a) $\alpha\beta = \iota_A d_1 d_2$.

(b) $\alpha^j = \iota_A d_1^j$ *for all* $j \in \mathbb{Z}$.

(c) $|\alpha| = |d_1|$, *where* $|\alpha|$ *and* $|d_1|$ *are the orders of* α *and* d_1 *in* H_A *and* D_n *respectively.*

Proof. To prove Lemma 2.1a, let α and β be defined as above. Then since ι_A is the identity in H_A, $\alpha\beta = (\iota_A d_1)(\iota_A d_2) = ((\iota_A d_1)\,\iota_A)\,d_2 = (\iota_A d_1)\,d_2 = \iota_A d_1 d_2$. The proof of Lemma 2.1b is a simple application of Lemma 2.1a using induction and the fact that $\alpha^{-1} = \iota_A d_1^{-1}$. To prove Lemma 2.1c, suppose that $|\alpha| = m$. Then m is the smallest positive integer such that $\alpha^m = \iota_A$. From Lemma 2.1b, $\alpha^m = \iota_A d_1^m$, so $\iota_A = \iota_A d_1^m$. We have assumed that $|A| > 2$, so ι_A can be extended to a unique element of D_n. Since $\iota_A \iota_P = \iota_A$, the uniqueness of extension gives $d_1^m = \iota_P$. If $d_1^\ell = \iota_P$ for some $\ell < m$, then $\alpha^\ell = \iota_A d_1^\ell = \iota_A \iota_P = \iota_A$, which contradicts the minimality of m. Thus m is the smallest positive integer such that $d_1^m = \iota_P$. Therefore $|d_1| = m$. □

It should be noted that in general, for $d \in D_n$, $\iota_A d$ is not necessarily an element of H_A. For any $d \in D_n$, let $d|_A$ denote the function d with the domain of d restricted to A, and let $d|_A(A)$ denote the image of A under this mapping. Then $\iota_A d \in S$ is an element of H_A if and only if $d|_A(A) = A$. In this light, we can express H_A as

$$H_A = \{\iota_A d \mid d \in D_n \text{ and } d|_A(A) = A\}. \tag{1}$$

There is a subtlety in this notation that is worth mentioning. Equation (1) for H_A is guaranteed to be valid if $|A| > 2$, but may fail otherwise. For example, suppose that $|A| = 1$. Then P_A is a point, so clearly H_A contains only the identity ι_A. But the set $\{\iota_A d \mid d \in D_n \text{ and } d|_A(A) = A\}$ contains two elements, the identity in D_n and the reflection of P about the line through the vertex in A. We use the useful notation of Equation (1) freely, since we have assumed that $|A| > 2$.

It is evident from Lemma 2.1a that composition within maximal subgroups is essentially the same as composition in D_n. As groups then, it is not surprising that many properties of the maximal subgroups of S are consequences of properties of D_n (with Lemma 2.1c as just one example). Another important property of D_n that is reflected in maximal subgroups of S is the structure of cyclic subgroups. Such subgroups are important to this discussion since both dihedral and cyclic groups contain them. As mentioned in Section 1, the subgroup of all rotations in D_n is the cyclic group of order n generated by a rotation, ρ, of $2\pi/n$ radians. As a result, the subgroup of all rotations in any maximal subgroup of S is also a cyclic group generated by a rotation.

Lemma 2.2. *Let* H_A *be a maximal subgroup with a nontrivial rotation. Then the subgroup of all rotations in* H_A *is a cyclic group generated by some rotation* $\alpha \in H_A$ *such that* $\alpha = \iota_A \rho^k$, *where* k *divides* n. *In particular, the subgroup of all rotations in* H_A *is isomorphic to* $\mathbb{Z}_{n/k}$, *where* k *is the smallest positive integer such that* $\iota_A \rho^k \in H_A$.

Proof. Assume H_A has a nontrivial rotation γ. Then $\gamma = \iota_A \rho^j$ for some j. Since the set $\{m \mid \iota_A \rho^m \in H_A, m \geq 1\}$ is thus nonempty, by the well-ordering principle it has a least element k. Hence there exists $\alpha \in H_A$ such that $\alpha = \iota_A \rho^k$. By the division algorithm, there exist unique $q, r \in \mathbb{N}$ such that $n = kq + r$ with $0 \leq r < k$. So

$$\iota_A \rho^r = \iota_A \rho^{n-kq} = \iota_A \rho^n \rho^{-kq} = \iota_A \iota_P \rho^{-kq} = \iota_A \rho^{-kq} = \left(\iota_A \rho^k\right)^{-q} = \alpha^{-q},$$

and $\alpha^{-q} \in H_A$ by closure. Thus $r = 0$ by minimality of k. Therefore k divides n.

It remains to be shown that the subgroup of all rotations in H_A is exactly $\langle\alpha\rangle$. To this end, let β be a nontrivial rotation in H_A. Then $\beta = \iota_A \rho^m$ for some m. Applying the division algorithm again, there exist unique $s, t \in \mathbb{N}$ such that $m = ks + t$, with $0 \leq t < k$. Then

$$\iota_A \rho^t = \iota_A \rho^{m-ks} = \left(\iota_A \rho^m\right) \rho^{-ks} = \beta \rho^{-ks} = \beta \iota_A \left(\rho^k\right)^{-s} = \beta \left(\iota_A \rho^k\right)^{-s} = \beta \alpha^{-s} \in H_A.$$

So t must be zero, by minimality of k. Thus $\beta = \iota_A \rho^{ks} = \left(\iota_A \rho^k\right)^s = \alpha^s \in \langle\alpha\rangle$.

From Lemma 2.1c, $|\langle\alpha\rangle| = \left|\iota_A \rho^k\right| = \left|\rho^k\right|$. And $\left|\rho^k\right| = n/k$ since k divides n. So $\langle\alpha\rangle \approx \mathbb{Z}_{n/k}$. □

Though Lemma 2.2 is useful for describing the cyclic subgroups of maximal subgroups as groups, it says nothing about what the subpolygons look like that have such subgroups. To aid in the description of these subpolygons, a distance function is defined on $V(P)$ that exploits the regularity of P and is independent of the actual size of the regular polygon.

Definition. The *polygonal distance* between two vertices v and w is the fewest number of edges between v and w in the regular polygon P. The polygonal distance is denoted $P(v, w)$.

The polygonal distance is equivalent to the usual Euclidean distance in the sense that for any vertices v_1, v_2, w_1, w_2, $P(v_1, w_1) = P(v_2, w_2)$ if and only if $E(v_1, w_1) = E(v_2, w_2)$, where $E(v, w)$ denotes the Euclidean distance between v and w. This follows immediately from the fact that P is a regular polygon. In particular, since the elements of D_n are isometries, we know $E(v, w) = E(vd, wd)$ for all $d \in D_n$. This implies

$$P(v, w) = P(vd, wd), \quad \text{for all } d \in D_n. \tag{2}$$

Further, since P is a regular polygon, a subpolygon P_A is regular if and only if there exists an $\ell \in \mathbb{N}$ such that for all $v, w \in A$ that are connected by an edge in P_A, the polygonal distance $P(v, w) = \ell$. So the vertices of any subpolygon which is itself a regular polygon must be evenly spaced around P with respect to the polygonal distance. The vertex sets of regular subpolygons are fundamental to describing the maximal subgroups of S, so we give these sets of vertices their own notation.

Definition. Let k divide n such that $k \neq n/2$. The k class of the vertex v_i, denoted by $[v_i]_k$, is defined as $[v_i]_k = \{v_j \mid P(v_i, v_j) = mk \text{ for some } m \in \mathbb{N}\}$.

From the discussion above, these k classes are precisely the vertex sets of regular subpolygons. Since $P(v_i, v_i\rho^{\ell k})$ is a multiple of k for all $\ell \in \mathbb{N}$, it is apparent that $v_j \in [v_i]_k$ if and only if $v_i\rho^{mk} = v_j$ for some $m \in \mathbb{N}$. So $[v_i]_k = \{v_i\rho^{mk} \mid m \in \mathbb{N}\}$. The set $\{v_i\rho^{mk} \mid m \in \mathbb{N}\}$ is the set of all vertices that v_i is mapped to under elements of $\langle\rho^k\rangle$, called the *orbit* of v_i under $\langle\rho^k\rangle$. No two distinct elements of $\langle\rho^k\rangle$ map v_i to the same vertex, so $|[v_i]_k| = |\langle\rho^k\rangle| = n/k$. So, each k class forms a regular subpolygon with n/k vertices (we have disallowed $k = n/2$ to ensure each k class has more than two vertices). Moreover, it is well known that the set of all orbits of any set under some group is a partition of that set, so $P_{[v]_k}$ is the unique regular subpolygon with n/k vertices containing v. Since the symmetry group of a regular polygon is dihedral, we have proven the following result:

Proposition 2.1. *Let P be a regular polygon with n sides. Then S has a maximal subgroup isomorphic to the dihedral group $D_{n/k}$ for every k which divides n.*

Dihedral maximal subgroups are thus abundant in the sense that as long as n is not prime (and P is not a square), S contains at least one nontrivial dihedral maximal subgroup (the trivial case being the group of symmetries of P). In contrast, the restriction that n be not prime is not sufficient to show that S contains a nontrivial cyclic maximal subgroup. As we will show, stronger restrictions must be placed on the divisors of n to guarantee nontrivial cyclic maximal subgroups of S exist.

We will use k classes to describe all subpolygons that have rotational symmetry.

Lemma 2.3. *A maximal subgroup H_A has a nontrivial subgroup of rotations if and only if*

$$A = \bigcup_{v \in A_0} [v]_k \text{ for some } k \text{ and some } A_0 \subseteq V(P).$$

Moreover, any nontrivial subgroup of rotations in H_A is isomorphic to $\mathbb{Z}_{n/h}$ for some h.

Proof. First, assume H_A has a nontrivial rotation. Then there exists $\alpha \in H_A$ such that $\alpha = \iota_A\rho^k$ for some k. Since $\iota_A\rho^k \in H_A$, we have $[v]_k \subseteq A$ for all $v \in A$. Let A_0 be a subset of A consisting of a representative of each k class. Then $A = \bigcup_{v \in A_0} [v]_k$.

For the other direction, assume $A = \bigcup_{v \in A_0} [v]_k$ for some k and some $A_0 \subseteq V(P)$. Since for any $v \in A$ the set $[v]_k$ is the orbit of v under ρ^k, we know $v\rho^k \in A$. Thus $\alpha = \iota_A\rho^k$ is an element of H_A. Since ρ^k is a nontrivial rotation in D_n, α is a nontrivial rotation in H_A. Therefore $\langle\alpha\rangle$ is a nontrivial subgroup of rotations of H_A.

From Lemma 2.1c, $|\alpha| = \left|\rho^k\right| = n/k$. Since $|\alpha| = |\langle\alpha\rangle|$, the cyclic group $\langle\alpha\rangle$ is of order n/k, and is therefore isomorphic to $\mathbb{Z}_{n/k}$. □

These k classes can then be viewed as the building blocks for all cyclic and dihedral maximal subgroups since both contain subgroups of rotations. However, at this point we have no way of knowing whether a subpolygon formed by a union of more than one k class will have a cyclic or a dihedral symmetry group. The following lemma gives one method of proving or disproving that a maximal subgroup is cyclic:

Lemma 2.4. *Let A be a collection of vertices of P that can be written as a union of k classes, with k the smallest positive integer such that $A = \bigcup_{v\in A_0}[v]_k$ for some set of vertices A_0. Then $H_A \approx \mathbb{Z}_{n/k}$ if and only if H_A contains no reflections. Otherwise, $H_A \approx D_{n/k}$.*

Proof. First note that since k is the smallest positive integer such that A can be written as the union of k classes, k is also the smallest positive integer such that $\iota_A\rho^k \in H_A$. So, by Lemma 2.2, the subgroup of all rotations in H_A is isomorphic to $\mathbb{Z}_{n/k}$. So clearly if $H_A \approx \mathbb{Z}_{n/k}$ then every element in H_A is a rotation. Conversely, if H_A contains no reflections, then it must contain only rotations. Since the set of all rotations in H_A is $\left\langle\iota_A\rho^k\right\rangle$, we have $H_A = \left\langle\iota_A\rho^k\right\rangle \approx \mathbb{Z}_{n/k}$.

If $H_A \not\approx \mathbb{Z}_{n/k}$, then $\mathbb{Z}_{n/k}$ is still the subgroup of all rotations in H_A. So H_A must contain some element $\gamma \notin \mathbb{Z}_{n/k}$. This implies that H_A is not cyclic. Since all finite plane symmetry groups are either cyclic or dihedral, H_A is thus isomorphic to a dihedral group. The only dihedral group that contains $\mathbb{Z}_{n/k}$ as its largest cyclic subgroup is $D_{n/k}$. Therefore $H_A \approx D_{n/k}$. □

So, we can now state the problem of finding cyclic maximal subgroups as follows: for which values of n can we find a collection of k classes, A, such that H_A contains no reflections?

We begin this search by constructing some subpolygons with cyclic symmetry groups. In order to construct such subpolygons we make use of the concept of an integer partition. A partition of an integer m is a way of expressing m as the sum of positive integers. Each summand in the expression of m is called a part of the partition. The usual convention dictates that the parts of a partition be written in nonincreasing order, but for our purposes this requirement is irrelevant. For our construction we will need the following definitions:

Definition. Let A and B be collections of vertices of P.

(a) Two vertices of A are said to be adjacent in P_A if they are connected by an edge in the subpolygon P_A.

(b) Let $B \subseteq A$. If for all $v \in B$ there exists $w \in B$ such that v is adjacent to w in P_A, then B is said to be a consecutive subset of A.

(c) The set $\mathscr{E}_A$ is defined by $\mathscr{E}_A = \{P(v_i, v_j) \mid v_i, v_j \in A$ and v_i is adjacent to v_j in $P_A\}$.

Note that the polygonal distance always refers to the minimum number of edges of the original polygon P between two vertices, even in reference to two vertices of a subpolygon. Note also that vertices labeled with consecutive indices, for example w_1 and w_2, are always meant to be adjacent in P_A.

Theorem 2.1. *Let k divide n. Then for every partition of k into m distinct parts, with $m \geq 3$, there exists a cyclic maximal subgroup of S isomorphic to $\mathbb{Z}_{n/k}$.*

Proof. Let k divide n. Suppose $k = a_1 + a_2 + \ldots + a_m$, for some $m \geq 3$, where all the a_i are distinct. Using this partition of k, we wish to construct a set of vertices A that will give rise to a subpolygon P_A with only rotations in its symmetry group H_A. To do this, let $A_0 = \{v_{i_1}, v_{i_2}, \ldots, v_{i_m}\}$ be a set of vertices such that $P(v_{i_j}, v_{i_{j+1}}) = a_j$ for all $j = 1, 2, \ldots, m-1$. Consider the set $A = \bigcup_{v \in A_0} [v]_k$. For convenience, let $A = \{w_1, w_2, \ldots, w_q\}$, where the first m vertices in A are precisely the elements of A_0, and $q = mn/k$. We break up the proof that $H_A \approx \mathbb{Z}_{n/k}$ into three parts.

(a) The set A has the following properties:

(i) $\mathscr{E}_A = \{a_i \mid i = 1, 2, \ldots, m\}$.

(ii) If B is any consecutive subset of A, and $|B| \leq m + 1$, then all elements of $\mathscr{E}_B$ are distinct.

We know from the construction of A that

$$P\,(w_i, w_{i+1}) = a_i \quad \text{for } i = 1, 2, \ldots, m-1.$$

Also, since $w_{m+1} = w_1 \rho^k$, we have $P(w_1, w_{m+1}) = k$. Since the set

$$\{w_1, w_2, \ldots, w_{m+1}\}$$

is a consecutive subset of A we may write

$$P(w_1, w_{m+1}) = P(w_1, w_m) + P(w_m, w_{m+1}).$$

So

$$\begin{aligned} P(w_m, w_{m+1}) &= P(w_1, w_{m+1}) - P(w_1, w_m) \\ &= k - (a_1 + a_2 + \ldots + a_{m-1}) \\ &= a_m. \end{aligned}$$

This shows that $\mathscr{E}_{A_0} = \{a_i \mid i = 1, 2, \ldots, m\}$. Now let $w_j \in A$. Then there exists an $\ell \in \mathbb{N}$ such that $w_j = w_i \rho^{\ell k}$ for some $w_i \in A_0$ by the construction of A. So (recalling Equation (2)),

$$P(w_j, w_{j+1}) = P(w_i\rho^{\ell k}, w_{i+1}\rho^{\ell k}) = P(w_i, w_{i+1}) = a_i,$$

which proves the first property.

To prove the second, note if B is consecutive subset of A and $|B| \leq m+1$, then $\mathscr{E}_B$ has at most m elements. Each element of $\mathscr{E}_B$ must be a unique part of the partition of k, all of which are distinct.

(b) The subgroup of all rotations in H_A is isomorphic to $\mathbb{Z}_{n/k}$:

In order to show that the subgroup of all rotations in H_A is $\mathbb{Z}_{n/k}$, from Lemma 2.2 we need only show that k is the smallest positive integer such that $\iota_A\rho^k \in H_A$. Assume, rather, that $\iota_A\rho^j$ is an element of H_A for some j such that $0 < j < k$. Let $A_1 = A_0 \cup \{w_{m+1}\}$. Note that since $|A_1| = m+1$, every element of $\mathscr{E}_{A_1}$ is unique by Theorem 2.1a-ii. Also note that since $\iota_A\rho^j$ is a rotation, it preserves both adjacency and orientation of the vertices of A. With these two facts, we see that $w_1\rho^j$ and $w_2\rho^j$ cannot both lie in A_1. If they did, we would have $P(w_1, w_2) = P(w_1\rho^j, w_2\rho^j) \in \mathscr{E}_{A_1}$, contradicting Theorem 2.1a-ii. But recall that $P(w_1, w_1\rho^j) = j$, and by construction, $P(w_1, w_{m+1}) = k$. Since $j < k$, this implies that $w_1\rho^j = w_s$ for some $w_s \in A_1$. Since the vertices of A are indexed clockwise, we have that $s < m+1$. Now, since $w_1\rho^j = w_s$, and ρ^j is orientation preserving, we may write $w_2\rho^j = w_{s+1}$. From our argument above, since $w_1\rho^j \in A_1$, we know that $w_2\rho^j \notin A_1$. That is, $s+1 > m+1$. Since we have already established that $s < m+1$, we have $s < m+1 < s+1$. This is impossible since both m and s are positive integers. Thus, k is the smallest positive integer such that $\iota_A\rho^k \in H_A$. Therefore, the subgroup of all rotations in H_A is isomorphic to $\mathbb{Z}_{n/k}$.

(c) H_A contains no reflections: We again proceed by contradiction. Suppose that P_A is symmetric about some line L. Let $d \in D_n$ be the reflection of P about L. Then $\alpha = \iota_A d \in H_A$. There are two cases to consider.

(i) L passes through some vertex $w_i \in A$. Let $B = \{w_{i-1}, w_i, w_{i+1}\}$. Now, $w_i\alpha = w_i$, and $w_{i+1}\alpha = w_{i-1}$. Moreover, from Theorem 2.1a-i,

$$P(w_i, w_{i+1}) = P(w_i\alpha, w_{i+1}\alpha) = P(w_i, w_{i-1}) = a_j \text{ for some } j.$$

But $P(w_{i-1}, w_i)$, $P(w_i, w_{i+1}) \in \mathscr{E}_B$, and B is a consecutive subset of A of order 3. Since $m \geq 3$, $|B| = 3 < m+1$. So $P(w_{i-1}, w_i)$ and $P(w_i, w_{i+1})$ must be distinct by Theorem 2.1a-i, which is a contradiction.

(ii) L passes through no vertices of A. Then there exists $w_i \in A$ such that $w_i\alpha = w_{i+1}$ and $w_{i-1}\alpha = w_{i+2}$. Thus, from Theorem 2.1a-i:

$$P(w_i, w_{i-1}) = P(w_i\alpha, w_{i-1}\alpha) = P(w_{i+1}, w_{i+2}) = a_j \quad \text{for some } j.$$

Let $B = \{w_{i-1}, w_i, w_{i+1}, w_{i+2}\}$. Then B is a consecutive subset of order 4. Since $m \geq 3$, $|B| \leq m + 1$. But clearly not every element of $\mathscr{E}_B$ is distinct. By Theorem 2.1a-ii, this is impossible.

Therefore, the subpolygon P_A has no line of symmetry. Thus H_A contains no reflections. The theorem now follows. □

Corollary 2.1. *If k divides n and $k \geq 6$, then S has a maximal subgroup isomorphic to $\mathbb{Z}_{n/k}$.*

Proof. Let k divide n and $k \geq 6$. Then $k = 1 + 2 + (k - 3)$, and $k - 3 > 2$, so k can be partitioned into at least 3 distinct parts. Thus by Theorem 2.1, S contains a maximal subgroup isomorphic to $\mathbb{Z}_{n/k}$. □

As an example of the construction of subpolygons with cyclic symmetry groups given in Theorem 2.1, let $n = 24$ and $k = 8$. Consider the partition $8 = 1+2+5$. Now let $A_0 \subseteq V(P)$ such that $A_0 = \{v_1, v_2, v_4\}$ (see Figure 1). Note that $P(v_1, v_2) = 1$ and $P(v_2, v_4) = 2$. If we then consider the set $A = \bigcup_{v \in A_0} [v]_8$, we get

$$\begin{aligned} A &= [v_1]_8 \cup [v_2]_8 \cup [v_4]_8 \\ &= \{v_1, v_9, v_{17}\} \cup \{v_2, v_{10}, v_{18}\} \cup \{v_4, v_{12}, v_{20}\} \\ &= \{v_1, v_2, v_4, v_9, v_{10}, v_{12}, v_{17}, v_{18}, v_{20}\}. \end{aligned}$$

So A is essentially made up of 3 copies of A_0 evenly spaced around the polygon, and one can see that the polygonal distances between adjacent vertices in P_A are all elements of the partition of k. The entire subpolygon in Figure 1 is P_A.

We have shown that, given a regular polygon with n sides and a positive integer $k \geq 6$ that divides n, we can construct a subpolygon with symmetry group $\mathbb{Z}_{n/k}$.

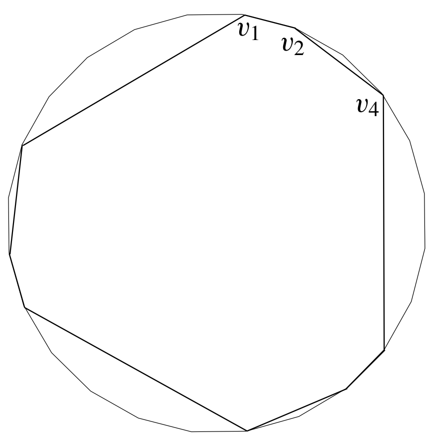

Figure 1. Subpolygon with symmetry group $\mathbb{Z}_3$ in a regular 24-gon.

With the following three results, we show that if $k < 6$ then no such subpolygon exists.

Lemma 2.5. *If A is the union of exactly two k classes, then H_A is isomorphic to a dihedral group.*

Proof. Let $A = [v]_k \cup [w]_k$, where $[v]_k \cap [w]_k = \varnothing$. If $[v]_k \cup [w]_k = [v]_j$ for some j, then P_A is regular and the result holds. So assume that is not the case. We know there exists some reflection $d \in D_n$ such that $vd = w$ and $wd = v$. Recall that $P_{[v]_k}$ and $P_{[w]_k}$ are the unique regular subpolygons with n/k vertices containing v and w respectively. Since d is an isometry, the subpolygon formed by the vertex set $d([v]_k)$ must also be a regular n/k-gon. Since $vd = w \in [w]_k$, we have $d([v]_k) = [w]_k$ by the uniqueness of $P_{[w]_k}$. Similarly $d([w]_k) = [v]_k$. So $d|_A(A) = A$, and $\iota_A d$ is a reflection in H_A. From Lemma 2.4, since A is the union of k classes and H_A contains a reflection, H_A is isomorphic to a dihedral group. □

Lemma 2.6. *For any $A \subseteq V(P)$, let $A^c = V(P) \setminus A$. If A is a subset of $V(P)$ such that $|A| > 2$ and $|A^c| > 2$, then $H_A \approx H_{A^c}$.*

Proof. Let A be a subset of $V(P)$ such that $|A| > 2$ and $|A^c| > 2$. Recall from Equation (1) that $H_A = \{\iota_A d \mid d \in D_n \text{ and } d|_A(A) = A\}$. Let

$$D_n(A) = \{d \in D_n \mid d|_A(A) = A\} \quad \text{and} \quad D_n(A^c) = \left\{d \in D_n \mid d|_{A^c}(A^c) = A^c\right\}.$$

Since all mappings in D_n are bijections from $V(P)$ to $V(P)$, we have $d|_A(A) = A$ if and only if $d|_{A^c}(A^c) = A^c$. So $D_n(A) = D_n(A^c)$. Now define the mapping $\phi : H_A \to H_{A^c}$ by $\phi(\iota_A d) = \iota_{A^c} d$. Such a mapping is guaranteed to exist since $D_n(A) = D_n(A^c)$, and furthermore, the same equality shows that ϕ maps onto H_{A^c}. Since $|A| > 2$, every element of H_A can be extended to a unique element of D_n. So $\iota_A d_1 = \iota_A d_2$ if and only if $d_1 = d_2$, and ϕ is thus well defined. To see that ϕ is one-to-one, suppose that $\phi(\iota_A d_1) = \phi(\iota_A d_2)$. Then $\iota_{A^c} d_1 = \iota_{A^c} d_2$. By assumption, $|A^c| > 2$, so uniqueness of extension gives $d_1 = d_2$. Thus $\iota_A d_1 = \iota_A d_2$. It follows from Lemma 2.1a that for any $d_1, d_2 \in D_n(A)$,

$$\phi((\iota_A d_1)\,(\iota_A d_2)) = \phi(\iota_A d_1 d_2) = \iota_{A^c} d_1 d_2 = (\iota_{A^c} d_1)\,(\iota_{A^c} d_2) = \phi(\iota_A d_1)\,\phi(\iota_A d_2)\,.$$

So ϕ is a homomorphism, and $H_A \approx H_{A^c}$. □

Lemma 2.7. *Let k divide n, $k \leq 5$, and $k \neq n/2$. Then S has no maximal subgroup isomorphic to $\mathbb{Z}_{n/k}$.*

Proof. Let k be as described and $A \subseteq V(P)$ such that A is the union of m k classes. Since $k \leq 5$, we know $m \leq 5$. Then we can write A^c as the union of $(k-m)$ k classes. Since $k \neq n/2$, both A and A^c have more than two elements. Since $m + (k-m) = k \leq 5$, either $m \leq 2$ or $k - m \leq 2$. Thus from Lemma 2.5, H_A or H_{A^c} is isomorphic to a dihedral group. From Lemma 2.6, $H_A \approx H_{A^c}$, so both

H_A and H_{A^c} are isomorphic to a dihedral group. Thus the symmetry group of any subpolygon whose vertices are the union of k classes is dihedral. So $\mathbb{Z}_{n/k}$ does not occur as a maximal subgroup of S. $\square$

We now have all of the information necessary to determine exactly for which regular polygons P, $S(P)$ contains cyclic maximal subgroups other than $\mathbb{Z}_1$ and $\mathbb{Z}_2$.

Theorem 2.2. *Let P be a regular polygon with n sides. Then S contains a maximal subgroup isomorphic to $\mathbb{Z}_m$, for some $m \geq 3$, if and only if $n = km$ for some $k \geq 6$. In particular,* 18 *is the smallest value of n for which this occurs.*

Proof. Suppose that S contains a cyclic maximal subgroup isomorphic to $\mathbb{Z}_m$ for some $m \geq 3$. Then, by Lemma 2.3, $m = n/k$ for some k. Since $m \geq 3$, we know that $k \neq n/2$. Then by the contrapositive of Lemma 2.7, since $\mathbb{Z}_m = \mathbb{Z}_{n/k}$ is a maximal subgroup of S, then $k \geq 6$. Thus $n = km$ where $k \geq 6$ and $m \geq 3$.

Conversely, suppose $n = km$ for some k and m such that $k \geq 6$ and $m \geq 3$. By Corollary 2.1, since $k \geq 6$ and k divides n, S contains a maximal subgroup isomorphic to $\mathbb{Z}_{n/k} = \mathbb{Z}_m$. The result follows since $|\mathbb{Z}_m| = m \geq 3$.

Thus $6 \times 3 = 18$ is the fewest number of vertices of a regular polygon P such that S has a cyclic maximal subgroup with more than two elements. $\square$

For values of $n \leq 40$, the only n for which S contains a nontrivial (other than $\mathbb{Z}_1$ and $\mathbb{Z}_2$) cyclic maximal subgroup are 18, 21, 24, 27, 28, 30, 32, 33, 35, 36, 39, and 40. In contrast, there are 26 values of $n \leq 40$ for which S contains a nontrivial dihedral maximal subgroup.

The case where n is even and $k = n/2$ was ignored throughout the paper in order to ensure that each individual k class formed a regular polygon with at least 3 vertices. However, the consequences of allowing k to take the value of $n/2$ are nontrivial. If $k = n/2$, then any subpolygon formed by exactly one k class is simply a line segment connecting two antipodal vertices, so its symmetry group is $\mathbb{Z}_2$. But suppose that we take the union of two k classes of adjacent vertices, $[v_1]_k$ and $[v_2]_k$. Then the resulting subpolygon is a nonsquare rectangle (if $n > 4$). The symmetry group of a nonsquare rectangle contains 4 elements: the identity, one rotation of order 2, and two reflections. This symmetry group is known by more than one name, including the Klein four group, and $\mathbb{Z}_2 \times \mathbb{Z}_2$. But if we define the dihedral groups in terms of generators and relations as $D_n = \langle d_1, d_2 \mid d_1^2 = d_2^2 = (d_1 d_2)^n = \iota_P \rangle$, then the symmetry group of a nonsquare rectangle is seen to be isomorphic to D_2 [Gallian 2002, p. 442]. This maximal subgroup exists only for all even $n > 4$ (using the construction above).

With this final case considered, we have characterized all maximal subgroups of S for any regular polygon P.

n	Dihedral maximal subgroups	Cyclic maximal subgroups
4	D_4	$\mathbb{Z}_1$, $\mathbb{Z}_2$
8	D_2, D_4, D_8	$\mathbb{Z}_1$, $\mathbb{Z}_2$
13	D_{13}	$\mathbb{Z}_1$, $\mathbb{Z}_2$
18	D_2, D_3, D_6, D_9, D_{18}	$\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$
24	D_2, D_3, D_4, D_6, D_8, D_{12}, D_{24}	$\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$
30	D_2, D_3, D_5, D_6, D_{10}, D_{15}, D_{30}	$\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$

Table 1. Maximal subgroups for various values of n.

Theorem 2.3. *Let P be a regular polygon with n sides, and let $n > 4$. Let S be the semigroup of partial symmetries of P. Then every maximal subgroup of S is isomorphic to one of the following groups, and S contains a maximal subgroup isomorphic to each of the following*:

(a) $\mathbb{Z}_1$;

(b) $\mathbb{Z}_2$;

(c) $D_{n/k}$ *for all k that divide n*;

(d) $\mathbb{Z}_{n/k}$ *for all k that divide n such that $k \geq 6$ and $n/k \geq 3$.*

Table 1 shows exactly which maximal subgroups occur for a variety of values of n.

Acknowledgement

This work was conducted by Tom Shelly as an undergraduate research project under the guidance of Dr. Janet Mills.

References

[Gallian 2002] J. A. Gallian, *Contemporary Abstract Algebra*, Houghton Mifflin Company, Boston, 2002.

[Mills 1990a] J. E. Mills, "The inverse semigroup of partial symmetries of a convex polygon", *Semigroup Forum* **41**:2 (1990), 127–143. MR 91j:20158 Zbl 0704.20051

[Mills 1990b] J. E. Mills, "Inverse semigroups through groups", *Internat. J. Math. Ed. Sci. Tech.* **21**:1 (1990), 93–98. MR 1036371 Zbl 0693.20059

[Mills 1993] J. E. Mills, "Factorizable semigroup of partial symmetries of a regular polygon", *Rocky Mountain J. Math.* **23**:3 (1993), 1081–1090. MR 94j:20077 Zbl 0815.20064

Received: 2007-06-11 Accepted: 2007-11-01

shellyt@seattleu.edu *Department of Mathematics, 901 12th Ave., P.O. Box 222000, Seattle, WA 98122-1090, United States*

jemills@seattleu.edu *Department of Mathematics, 901 12th Ave., P.O. Box 222000, Seattle, WA 98122-1090, United States*