**M621, HW2, due Sept. 8: 9.11, Selected solutions.**

1. For the regular $n$-gon: let $r$ be the $\frac{360}{n}$ rotation in the clockwise direction, let $u$ be a reflection of the regular $n$-gon, let $s$ be the reflection through the line of symmetry of the regular $n$-gon that passes through 1 and the center of the regular $n$-gon, and let $e$ be the identity element of $D_{2n}$, the identity function.

   (a) For any $w \in D_{2n}$, let $Fix(w) = \{k \in \{1, \dots, n\} : w(k) = k\}$. Three examples: $Fix(r) = \emptyset$, $Fix(e) = \{1, \dots, n\}$, and if $n = 4$, and $s$ is the reflection through the line of symmetry of the square that passes through 1, then $Fix(s) = \{1, 3\}$.

      i. **Brief explanation.** If $n$ is odd, and $u$ is a reflection, what is $|Fix(u)|$? **Solution.** 1. Each line of symmetry is a line through a vertex $v$ , and the vertex $v$ is the only fixed point of the associated symmetry $u$.

      ii. **Brief explanation.** If $n$ is even, and $u$ is a reflection, what possibilities are there for $|Fix(u)|$? **Solution.** $|Fix(u)| = 2$, when the line of symmetry passes through a vertex and its antipodal vertex, and $|Fix(u)| = n$ when the associated line of symmetry is the perpendicular bisector of opposed edges of the n-gob.

      iii. **Brief explanation.** If $n > k > 0$, what is $|Fix(r^k)|$? **Solution.** $|Fix(r^k)| = n$—each vertex is moved (by $k$ positions).

      iv. It is clear that if $n > k \geq 0$, the rotation $r^k$ is completely determined by $r(1)$. In fact, for any $j \in \{1, \dots, n\}$, $r^k$ is completely determined by $r^k(j)$. For $j \in \{1, \dots, n\}$, what is $r^k(j)$? (Your answer will probably involve "mod n".)

      **Solution.** We'll define the function piecewise: Let $r^k(j) = k + j$, when $n > k + j$, and $r^k(j) = k + j + 1 \ mod \ n$, otherwise.

      (For example, if $n = 6, k = 3, j = 4$, then $r^3(4) = r(r^2)(4) = r(r(r(4)) = r(r(r^1(4) = r(r(5))$, using the first part of the "rule", and $r(r(5)) = r(r^1(5)) = r(6 + 1 \ mod \ 6) = r(1) = r^1(1) = 2$.)

      v. **Brief explanation.** Suppose $u$ is a reflection, explain why if $u$ is a reflection, then $u \neq r^k$ for any $n > k \geq 0$. (If $n$ is odd, each reflection has one fixed point, but if $n$ is even, there are reflections that have no fixed points. You'll want to make sure you deal with both of those cases.)

      **Solution.** $|Fix(r^k)| = 0$, so if $|Fix(u)| \neq 0$, $r^k \neq u$. If $|Fix(u)| = 0$, then $n$ is even, and the line of symmetry that determines $u$ is a perpendicular bisector of two opposite edges–notice that $k, k+1$ is one of those opposite edges, then $u(\{k, k+1\}) =$

$\{k, k+1\}$. On the other hand, the rotation $r^k$ maps the edge $\{k, k+1\}$ to some other edge, so $r^k \neq u$.

There are other explanations: For example, rotations are orientation-preserving, while reflections are orientation-reversing—though we haven't formally defined these the "orientation-preserving" notion yet.

vi. **Brief explanation.** Determine the following, briefly explaining for your answer. *We did* i-iv in class (and the class did well on the exercise), so I won't do this one.

vii. Comment briefly on the following: "Since $rs$ and $sr^{-1}$ agree on the vertices that make up an edge (namely 1 and 2), it follows that $rs = sr^{-1}$".

**Solution.** The statement is correct—since $rs$ and $sr^{-1}$ have the same effect on two vertices (namely 1 and 2) of an edge, the two symmetries are equal.

viii. For $n > 2$, show that $D_{2n}$ is not Abelian (by producing a pair of elements $y, z \in D_{2n}$ such that $yz \neq zy$).

**Solution.** It has been shown that $rs = sr^{-1}$. Thus $rs = sr$ implies $sr = sr^{-1}$, from which it follows (by cancellation) that $r^2 = e$, but then $1 = e(1)r^2(1) = 3$, contradicting that $n > 2$. It follows that $rs \neq sr$, so $D_{2n}$ is non-Abelian.

2. Suppose $G$ is a group, and for all $g \in G$, $g^2 = e$. Prove that $G$ is Abelian.

**Proof.** Suppose that $g^2 = e$ for all $g \in G$. Let $a, b \in G$. We have $e = (ab)^2 = abab$. Multiplying this equation on the left by $a$, and on the right by $b$, results in $ba = ab$. Since $a$ and $b$ are arbitrary elements in $G$, $G$ is Abelian.

3. **Short answer, but provide specifics.** Find a group $G$ such that for all $g \in G$, $g^3 = e$, but $G$ is not Abelian.

4. Suppose that $G$ is a group, $x, y$ are elements of $G$, $n \in \mathbb{N}$, and $(xy)^n = e$. Prove that $(yx)^n = e$. Suggestion: Find a power of $yx$ "inside" $(xy)^n$.

   **Proof.** Since $e = (xy)^n = x(yx)^{n-1}y$, it follows that $x^{-1}y^{-1} = (yx)^{-1}$. Multiply both sides of the last equation on the right by $yx$ leads to the equation $e = (yx)^n$, completing the proof.

5. Using exercise 4 directly above, prove that if $G$ is a group, $n \in \mathbb{N}$, then $|xy| = |yx|$. (Make sure you consider consider the possibility that one or both of $xy, yx$ have infinite order.)

   **Proof.** Exchanging the roles of $x$ and $y$ above, it follows that for any $n \in \mathbb{N}$ $(yx)^n = e$ implies that $(xy)^n = e$. Thus, for any $n \in \mathbb{N}$, $(xy)^n = e$ if and only if $(yx)^n = e$.

   Let $A = \{k \in \mathbb{N} : (xy)^k = e\}$, and let $B = \{j \in \mathbb{N} : (yx)^j = e\}$. By the paragraph above implies that $A = B$. Suppose $|xy|$ is finite. Then $A$ is non-empty, and $|xy|$ is the least element of $A$. Since $A = B$, $B$ is non-empty, and the least element of $B$ is $|yx|$, and is equal to the least element of $A$, which is $|xy|$. Thus, $|xy| = |yx|$.

   If $|xy| = \infty$, then $A$ is empty. If $A$ is empty, then $B$ is empty, which implies that $|yx| = \infty$, completing the proof.

   **Comment.** Here's a useful observation, one we've seen before. Let $G$ be a group having elements $y$ and $z$. Then $O_y = \{k \in \mathbb{N} : y^k = e\} = O_z = \{j \in \mathbb{N} : z^j = e\}$ if and only if $|y| = |z|$.

6. (Suggested, but voluntary, +1 EC—perhaps you'll have a chance to write it on the board next Thursday) Let $n \in \mathbb{N}$. Recall that $S_n$ is the group of permutations of $\{1, \ldots, n\}$. Let $\alpha, \beta$ be elements of $S_n$. Prove that $Fix(\beta\alpha\beta^{-1}) = \beta(Fix(\alpha)\}$.

   **Proof.** Suppose $z \in Fix(\beta\alpha\beta^{-1})$. So $\beta\alpha\beta^{-1}(z) = z$; hence, $\alpha(\beta^{-1}(z)) = \beta^{-1}(z)$. That is, $\beta^{-1}(z) \in Fix(\alpha)$, from which it follows that $z \in \beta(Fix(\alpha))$. Thus, $Fix(\beta\alpha\beta^{-1}) \subseteq \beta(Fix(\alpha))$. Now suppose $y \in \beta(Fix(\alpha))$. So $y = \beta(u)$, where $u \in Fix(\alpha)$. Now $\beta\alpha\beta^{-1}(\beta(u)) = \beta\alpha(u) = \beta(u)$, the right-most equality because $u \in Fix(\alpha)$. Apparently $y \in Fix(\beta\alpha\beta^{-1})$, and since $y$ is an arbitrarily selected element of $\beta(Fix(\alpha)$, it has been shown that $Fix(\alpha) \subseteq Fix(\beta\alpha\beta^{-1})$, completing the proof.