Math 541 Spring 2011
Solutions: HW#5, — Orthogonal symmetries of the n-regular polygon, Subgroups of $\mathbb{Z}$, Product, Cyclic groups

Remark. Answers should be written in the following format:
i) Statement and/or Result.
ii) Main points that will appear in your explanation or proof or computation.
iii) The actual explanation or proof or computation.

1. *Orthogonal symmetries of the n-regular polygon.* Consider the set $\mathcal{P}_n \subset \mathbb{R}^2$ with vertices at $\{(\cos(\theta), \sin(\theta))$; where $\theta = k \cdot 360/n,\ k = 0, 1, ..., n-1\}$. Denote by $D_n = Stab_{O(2,\mathbb{R})}(\mathcal{S})$, the group of orthogonal symmetries of $\mathcal{P}_n$. The group D_n is also called the Dihedral group of order n.

   (a) Show that $\#D_n = 2n$, and write explicitly the elements of D_n in term of rotations and reflections with respect to lines.

      1. *Main points.* A linear operator on $\mathbb{R}^2$ is defined uniquely by its application on two linearly independent vectors.
      2. *Solution.* Let $A \in D_n$. Since $A \in O$ it preserves angles up to a sign. So the the side with vertices at $(1, 0)$, $(\cos(360/n), \sin)$ must go to one of the others n sides with a possible flip (if the angle is changed from $360/n$ to $-360/n$) so we are done $2n$ options. Moreover, we have

$$D_n = \{r_0, r_{360/n}, r_{2\cdot 360/n}, ..., r_{(n-1)\cdot 360/n},\ \ s_{l_0}, s_{l_{\frac{1}{2}\cdot 360/n}}, ..., s_{l_{(n-1)\cdot\frac{1}{2}\cdot 360/n}}\},$$

         where the $r'_\theta s$, are the appropriate rotations, and the $s_{l_{\frac{k}{2}\cdot 360/n}}$, $k = 0, ..., n-1$ are the reflections with respect to the lines of slopes $\frac{k}{2} \cdot 360/n$, $k = 0, ..., n-1$. So we can conclude that $\#D_n = 2n$.

   (b) Write also matrices that describe these elements of D_n.

      1. Main points. We know the answer for all the rotations. All the reflections can be obtained using composition of one specific reflection and an appropriate rotation.
      2. *Answer.* A direct calculation shows that (remember that a linear transformation on $\mathbb{R}^2$ is completely determined by its action on two basis vectors):

$$s_{l_0} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad s_{l_{\frac{1}{2}\cdot 360/n}} = r_{360/n} \circ s_{l_0}, ..., \ s_{l_{\frac{1}{2}\cdot(n-1)\cdot 360/n}} = r_{(n-1)\cdot 360/n} \circ s_{l_0}.$$

2. *Subgroups of $\mathbb{Z}$.* Consider the group $(\mathbb{Z}, 0, +)$ of integers.

   (a) Show that for every $d \in \mathbb{N} = \{0, 1, 2, ...\}$ the set $d\mathbb{Z} = \{d \cdot n\ ;\ \ n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

1. *Main points.* Direct calculation.
2. *Proof.* Do it!

(b) Show the converse, if $H < \mathbb{Z}$ is a subgroup, then there exists an integer $d \geq 0$ such that $H = d\mathbb{Z}$. Hint: Use the Euclid theorem (ET)

If $m, n \in \mathbb{N}$, then there exist $q, r \in \mathbb{N}$ such that $n = qm + r$, with $0 \leq r < m$.

1. *Main points.* ET above.
2. *Proof.* Let $H < \mathbb{Z}$. If $H = \{0\}$ we are done. So we can assume that H contains positive integers. Let d be the smallest positive integer in H. We need to show that any other integer n in H is a multiple of d. We can assume that $n > 0$. By ET we have $q, r \geq 0$ so that

$$n = q \cdot d + r, \quad 0 \leq r < d.$$

In particular, $d > r = n - q \cdot d \in H$, so by the minimality assumption on d, we have $r = 0$.

3. *Product of groups.* Suppose G and H are groups. Consider the Cartesian product $G \times H$ with its natural multiplication

$$(g, h) \cdot (g', h') = (g \cdot g', h \cdot h'),$$

and identity element $(1_G, 1_H)$.

(a) Consider the sets $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$, $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ which are groups with addition + modulo 2, 3, and 6 respectively. Show that the map

$$\begin{array}{rcl} \varphi & : & \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3, \\ x & \mapsto & (x \mod 2, \quad x \mod 3), \end{array}$$

is an isomorphism.

1. *Main points.* Computation of the kernel.
2. *Proof.* Suppose $x \in \ker(\varphi)$. Then we can think on x as an integer, and since x is divisible by 2 and 3 it must be that also 6 divides x.

4. *Cyclic groups.* A group $(C, \cdot, 1)$ is called cyclic if there exist an element $x \in C$ such that $C = \{x^k;\ k \in \mathbb{Z}\}$, where

$$x^k = \begin{cases} \underbrace{x \cdot x \cdot \ldots \cdot x}_{k \text{ times}}, & \text{if } k > 0, \\ 1 \quad \text{if } k = 0, \\ \underbrace{x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}}_{-k \text{ times}}, & \text{if } k < 0. \end{cases}$$

(a) Show that the group $\mathbb{Z}$ is cyclic.

1. Here the operation $\cdot$ is the addition $+$, and $\mathbb{Z}$ is generated by 1.

(b) Show that for every integer $n \geq 1$ the group $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ with operation of addition + modulo n, is cyclic group of order n.

1. It is generated by 1.

(c) Show that the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

1. Every element is of order $2 : (x, y) + (x, y) = (0, 0)$. No element is of order 4.

(d) Let C be a cyclic group. Show that if C is of finite order n, i.e., $\#C = n$ for some positive integer n, then C is isomorphic to $\mathbb{Z}_n$. Show that if the cardinality of C is infinite, then C is isomorphic to $\mathbb{Z}$. Hint: Analyze the maps $\mathbb{Z}_n \to C$ given by $k \mapsto x^k$, and $\mathbb{Z} \to C$ given by $x \mapsto x^k$, where x is a generator of C.

1. *Main points.* The above hint.
2. *Proof.* Suppose $\#C = \infty$. Let us compute the kernel of the (onto!) homomorphism

$$\begin{aligned} \varphi &: \mathbb{Z} \to C, \\ \varphi(k) &= x^k. \end{aligned}$$

We have $\ker(\varphi) = \{0\}$. Indeed, if we had for $k > 0$, $x^k = 1$, then $x^{k+1} = x$, and we deduce the $\#C \leq k < \infty$. Next, suppose that $\#C = n$, then $C = \{1 = x^0, x, ..., x^{n-1}\}$. Now the map,

$$\begin{aligned} \varphi &: \mathbb{Z}_n \to C, \\ \varphi(k) &= x^k, \end{aligned}$$

is an isomorphism.

Remarks • I will be happy to help you understanding these answers. Please visit me in my office hours.

Good Luck!