Homework 3

Elliott Yoon

October 9, 2023

1 10/02

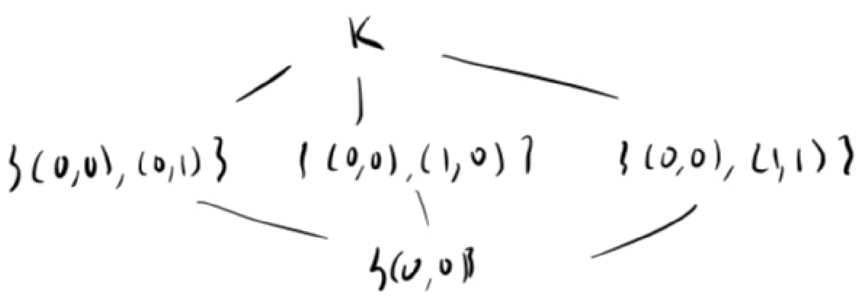
1. Show that if G is a group and $a \in G$ is an element satisfying $a^n = e$ for some integer $n \geq 1$, then the order of a divides n.

   - Let G be a group, $a \in G$ such that $a^n = e$ for some integer $n \geq 1$. Then $|a| < \infty$. Letting $m = |a|$, we have from the division algorithm that there exists unique $r, q \in \mathbb{Z}$ such that $n = mq + r, \quad 0 \leq r < m$. Then

     $$e = a^n = a^{mq+r} = a^{mq}a^r = (a^m)^q a^r = e \cdot a^r = a^r.$$

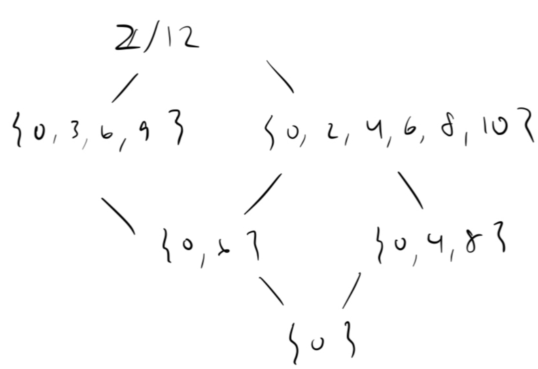
     Since $r < m$ and m is the smallest nonzero integer such that $a^m = e$, it must be the case that $r = 0$. Hence $n = mq$, so $|a| = m$ divides n. $\square$

2. Draw the lattice of subgroups for the group $K = \mathbb{Z}/2 \times \mathbb{Z}/2$.



   - $\square$

3. Draw the lattice of subgroupos for the group $\mathbb{Z}/12$.



   - $\square$

4. Using Example 6.12, find a cycle decomposition for $l(1\,2\,3)$.

   - Note that $l(1\,2\,3)$ is the function that maps the cycle $x \mapsto (1\,2\,3) \circ x$. Using the labeling of elements of S_3 in Example 6.12, we have that l maps:

$$\begin{aligned} e &\mapsto (1\,2\,3) \circ e = (1\,2\,3) & 1 &\to 5 \\ (1\,2) &\mapsto (1\,2\,3) \circ (1\,2) = (1\,3) & 2 &\to 3 \\ (1\,3) &\mapsto (1\,2\,3) \circ (1\,3) = (2\,3) & 3 &\to 4 \\ (2\,3) &\mapsto (1\,2\,3) \circ (2\,3) = (1\,2) & 4 &\to 2 \\ (1\,2\,3) &\mapsto (1\,2\,3) \circ (1\,2\,3) = (1\,3\,2) & 5 &\to 6 \\ (1\,3\,2) &\mapsto (1\,2\,3) \circ (1\,3\,2) & 6 &\to 1 \end{aligned}$$

   We can think of $l(1\,2\,3)$ as being an element of S_6 defined by the column on the right, i.e.

$$l(1\,2\,3) = (1\,5\,6)(2\,3\,4).$$

   □

2 10/04

1. Suppose G is a finite group of even order. Show there exists some $x \neq e$ in G with $x^2 = e$.

   - For each $g \in G$, we we can pair up g with its inverse $g^{-1} \in G$ if $g \neq g^{-1}$ (or equivalently $g^2 = e$). Notice that e is its own inverse and thus cannot be paired with another distinct element. With k pairs of elements and the identity e, we have seen $2k + 1$ elements so far. Since $|G|$ is even, there must exist another element $g' \in G$, $g' \neq e$ that is its own inverse such that $g^2 = e$. □

2. Show every finite group G of order 4 is either isomorphic to $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$.

   - Let $G = \{e, a, b, c\}$ be a finite group of order 4. We can assume from (10/04.1) that without loss of generality, $c^2 = e$. Considering the case where $a^{-1} = b$, we can easily check from the Cayley table that we have a binary operation built into G. Moreover, this Cayley table is the same as $\mathbb{Z}/4$ so $G \cong \mathbb{Z}/4$. Now, consider the case where $a^{-1} \neq b$. Then $a^{-1} = a$ and $b^{-1} = b$. The Cayley tables for this group structure and $\mathbb{Z}/2 \times \mathbb{Z}/2$ are identical, and thus $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. □

3. Show a finite group of order 5 is isomorphic to $\mathbb{Z}/5$.

   - We've seen in class that if G is a group and S a subgroup of G, then $|S|$ divides $|G|$. However, 5 is prime so the only subgroup of G is the trivial subgroup. Thus if $a \neq e \in G$, then $a \neq a^2 \neq a^3 \neq a^4 \neq a^5$ since any subgroup containing a must have order 5. So $G = \{a, a^2, a^3, a^4, a^5\}$ is cyclic. □

3 10/06

1. Say that an action of a group G on a set X is trivial if $g \cdot x = x$ for all $g \in G$ and x on X. Suppose that p is a prime and that X is a set with fewer than p elements. Show that all actions of $\mathbb{Z}/p$ on X are trivial.

   - Let k be an action of $\mathbb{Z}/p$ on X, and $a \in \mathbb{Z}/p$. Since p is prime, the set $\{0, a, \ldots, (p-1)a\}$ are all distinct. Furthermore, X has fewer than p elements, so the pigeonhole principle gives that there exists $0 \leq j < k < p$ such that

     $$ja(x) = ka(x)$$

     for $x \in X$. Notice that

     $$(k-j)a \cdot_k (ja \cdot_k x) = ja \cdot_k x,$$

     and similarly,

     $$i(k-j)a \cdot_k (ja \cdot_k x) = ja \cdot_k x,$$

     for every i. Recall that $\{0, (k-j)a, 2(k-j)a, \ldots, (p-1)(k-j)a\}$ are distinct. Now, for $x \in X$, by our previous observation, there exists $l, q \in \mathbb{N}$ distinct elements such that $la \cdot_k x = qa \cdot_k x$. Notice that $la \neq wqa$, thus $(la)^{-1}qa \neq 0$, so

     $$\left((la)^{-1}qa\right) \cdot_k x = (la)^{-1} \cdot_k (qa \cdot_k x) = (la)^{-1} \cdot_k (la \cdot_k x) = \left((la)^{-1}la\right) x = x.$$

     suffices to show every nonzero action is trivial. □

2. Compute the set $\mathrm{Hom}(\mathbb{Z}/2, S_4)$ of group homomorphisms into S_4. Use your computation to describe all group actions of $\mathbb{Z}/2$ on $\{1, 2, 3, 4\}$.

   - Note that $\mathbb{Z}/2\{0, 1\}$. Recall that from Lemma 5.5, any group homomorphism from $\mathbb{Z}/2$ must map $0 \mapsto e$. Further, any group homomorphism f from $\mathbb{Z}/2$ has

     $$f(0) = f(1+1) = f(1) \cdot f(1).$$

     Thus $f(1)$ must have order less than or equal to 2, i.e.

     $$f(1) \mapsto g \in \{e, (1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

     Moreover, each group homomorphism $f_g : \mathbb{Z}/2 \longrightarrow S_4$

     $$f_g = \begin{cases} 0 \mapsto e \\ 1 \mapsto g \in \{e, (1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \end{cases}$$

     uniquely defines a group action k_{f_g} associated to f_g. □