Math 335, Homework 5

Due Wednesday, March 10

Mark S Kim

---

1. Is the group D_4 (the group of symmetries of a square, under the operation of composition) cyclic? Carefully explain how you know.

   Answer:

   $$D_4 = \{I, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

   In order for D_4 to be cyclic, there must be an element of $d \in D_4$ such that $\langle d \rangle = D_4$. If we list all generators for D_4 we come up with the following:

   $$\begin{aligned} \langle I \rangle &= \{I\} \\ \langle R_{90} \rangle = \langle R_{270} \rangle &= \{I, R_{90}, R_{180}, R_{270}\} \\ \langle R_{180} \rangle &= \{I, R_{180}\} \\ \langle H \rangle &= \{I, H\} \\ \langle V \rangle &= \{I, V\} \\ \langle D \rangle &= \{I, D\} \\ \langle D' \rangle &= \{I, D'\}. \end{aligned}$$

   This shows that there is no $d \in D_4$ such that $\langle d \rangle = D_4$.

2. (a) Let $G = \langle a \rangle$ be a cyclic group in which $\mathrm{ord}(a) = \infty$. Prove that

   $$\langle a^k \rangle \subseteq \langle a^m \rangle$$

   if and only if $m|k$. (**Hint**: A problem from Homework 4 will be helpful here.)

   Proof. For the forward direction, let $\langle a^k \rangle \subseteq \langle a^m \rangle$, which said another way means that $x \in \langle a^k \rangle$ implies $x \in \langle a^m \rangle$. Suppose that $x = \left(a^k\right)^i$ for some $i \in \mathbb{Z}$, which implies that $x = (a^m)^j$ for some $j \in \mathbb{Z}$. Then,

   $$\begin{aligned} &a^{ki} = a^{mj}, \text{ for some } i, j \in \mathbb{Z},\ i \neq 0, \text{ and} \\ &ki = mj \text{ (proved in HW2).} \end{aligned}$$

   Recall that the division algorithm states

   $$k = mq + r, \quad 0 \leq r \leq (m-1), \quad q, r \in \mathbb{Z}.$$

   By substituting for k in the division algorithm, we find that $mqi + ri = mj$. But since $i \neq 0$ as stated earlier, r must be zero and $k = mj$ for some $j \in \mathbb{Z}$. By definition, we can conclude that $m|k$.

Conversely, let $m|k$. By definition, this means that $k = mp$ for some $p \in \mathbb{Z}$. Suppose $x \in \langle a^k \rangle$ for some $q \in \mathbb{Z}$. Then,

$$\begin{aligned} x &= \left(a^k\right)^q = a^{kq} \\ &= a^{mpq} = (a^m)^{pq} \end{aligned}$$

Hence $x \in \langle a^m \rangle$ and $\langle a^k \rangle \subseteq \langle a^m \rangle$. $\square$

(b) Give a counterexample to show that part (a) is false if $\text{ord}(a)$ is finite. (**Hint**: Try making m larger than the order of a.)

Answer:

Let $G = \langle 3 \rangle = \{0, 1, 2, 3\} = \mathbb{Z}_4$ under addition modulo 4. Then,

$$\begin{aligned} \langle a^k \rangle &= \langle 3 \cdot 2 \rangle = \langle 2 \rangle = \{0, 2\} \\ \langle a^m \rangle &= \langle 3 \cdot 3 \rangle = \langle 1 \rangle = \{0, 1, 2, 3\}. \end{aligned}$$

Notice that $\langle 3 \cdot 2 \rangle \subseteq \langle 3 \cdot 3 \rangle$, but 3 does not divide 2.

3. Let G be any group, and let $a \in G$ be an element of order 15. What is the order of a^6? Of a^{10}? Prove your answers.

Answer:

By saying that $\text{ord}(a) = 15$, we are saying that $k = 15$ is the least positive integer such that $a^k = e$. This also means that for all $k < 15$, $a^k \neq e$. To find the order of a^6, we can evaluate $\left(a^6\right)^n$ as follows:

$$\begin{aligned} \left(a^6\right)^1 &= a^6 \neq e \\ \left(a^6\right)^2 &= a^{12} \neq e \\ \left(a^6\right)^3 &= a^{18} = a^{15} \cdot a^3 = e \cdot a^3 = a^3 \neq e \\ \left(a^6\right)^4 &= a^{24} = e \cdot a^9 = a^9 \neq e \\ \left(a^6\right)^5 &= a^{30} = e^2 = e. \end{aligned}$$

This shows that $\text{ord}(a^6) = 5$ as any $n < 5$ does not produce the identity. Similarly, we can follow the previous steps to find that $\text{ord}(a^{10}) = 3$.

4. Consider the group $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ under addition modulo n. We say that an element k of this group *generates* $\mathbb{Z}_n$ if $\langle k \rangle = \mathbb{Z}_n$.

(a) List all of the elements of $\mathbb{Z}_9$ that generate $\mathbb{Z}_9$.

Answer:

All of the elements of $\mathbb{Z}_9$ that generate $\mathbb{Z}_9$ are: 1, 2, 4, 5, 7, and 8. ($\langle 1 \rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 8 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$)

(b) Prove that k generates $\mathbb{Z}_n$ if and only if $\gcd(n, k) = 1$.

Proof. Suppose that k generates the group $G = \mathbb{Z}_n$ under addition modulo n, which we know to be a cyclic group. By Theorem, $\text{ord}(k) = n$ (the number of elements in G). Furthermore, by yet another Theorem, $\text{ord}(k) = \frac{n}{\gcd(k,n)}$. Therefore if $\text{ord}(k) = n$, then it must be true that $\gcd(k, n) = 1$.

Conversely, suppose $\gcd(n, k) = 1$ and consider the cyclic group $G = \mathbb{Z}_n$ under addition modulo n. Given any subgroup $\langle k \rangle$, $\text{ord}(k) = \frac{n}{\gcd(k,n)} = n$, which is the number of elements in G. Since $\langle k \rangle$ contains all elements in $\mathbb{Z}_n$, it generates $\mathbb{Z}_n$ under addition modulo n. $\square$

5. Consider the group $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ under addition modulo p, where p is a prime number. What are all of the subgroups of $\mathbb{Z}_p$? Carefully explain how you know that you've found them all.

   Answer:

   The fundamental Theorem of Cyclic Groups states that there is exactly one subgroup of G with d elements – namely $\langle g^{n/d} \rangle$. Since n is a prime number p, only two divisors exist for p, which are exclusively 1 and p. Hence there are only two subgroups that exist for $\mathbb{Z}_p$, which are the trivial subgroup $\{0\}$ and the non-proper subgroup $\langle g \rangle = \mathbb{Z}_p$ under addition modulo p.