Assignment II

1. Let n be a positive integer. For each d dividing n, let $A_n(d)$ denote the set of all numbers between 1 and n whose GCD with n is d. □

   1. For $n = 24$ and values $d = 1, 2, 3, 4, 6, 12$ Find $A_n(d)$.
   2. Show that $\sum_{d|n} A_n(d) = \sum_{d|n} A_n(\frac{n}{d}) = n$.
   3. Let $1 \leq i \leq n$. Show that $i \in A_n(d)$ if and only if $GCD(\frac{i}{d}, \frac{n}{d}) = 1$. Hence conclude that the number of elements in $A_n(d)$ equals the number of integers between 1 and $\frac{n}{d}$ that are relatively prime to $\frac{n}{d}$. That is $|A_n(d)| = \phi(\frac{n}{d})$.
   4. Combining all the above, show that Show that $\sum_{d|n} \phi(d) = \sum_{d|n} \phi(\frac{n}{d}) = n$

2. Let $(H, +)$ and $(K, +)$ be two Abelian groups. We define the product $G = H \times K$ of the two groups as follows. Elements of G are elements in the cartitian product of H and K. That is, $G = \{(a, b)|a \in H, b \in K\}$. We define $+$ in G in the following (natural) way: $(a, b) + (a' + b') = (a + a', b + b')$. (Note here that $a + a$ is the result of adding a with a' in H and $b + b'$ is the result of adding b with b' in K.) Show that G defined this way is a group. What is the inverse of $(a + a', b + b')$? What is the identify element in G? □

3. Find the product group of $(\mathbf{Z_3}, +)$ and $(\mathbf{Z_4}, +)$. What is the sum of $(2, 3)$ and $(1, 1)$ in the product group? What is the inverse of the sum? □

4. Consider the multiplicative groups $\mathbf{Z_3}^*$ and $\mathbf{Z_4}^*$. Find the product of $(2, 3)$ and $(2, 2)$ in this group. What is the inverse of $(2, 2)$ in this group? □

5. Let H be a cyclic group of order m with generator a. Let K be a cyclic group of order n with generator b. Let G be their product group. □

   1. show that the element (a, b) has order $LCM(m, n)$
   2. Let i be a number between 1 and m and j be a number between 1 and n. Find a general formula for the order of the element (a^i, b^j).
   3. Find the order of the element $(3, 5)$ in the group $Z_{13} \times Z_{15}$
   4. Show that G is a cyclic group if and only if m and n are relative prime.

6. Let S be a subgroup of a group G. Let $a, b, x, y \in G$. Consider the cosets $a + S$ and $b + S$. □

   1. Suppose $x \in a + S$ and $y \in b + S$, then show that $(x + y) \in (a + b) + S$. (Hint: Remember that we proved in the class that $x \in a + S$ if and only if $x - a \in S$.)
   2. Hence conclude that if $a + S = x + S$ and $b + S = y + S$, then $(a + b) + S = (x + y) + S$.
   3. Consider the line (subgroup) $x + y = 0$ in the plane $\mathbf{R^2}$. Let us denote by S, the points in this line. Plot the cosets $(1, 1) + S, (0, 2) + S, (2, 2) + S$ and $(4, 0) + S$. Plot the cosets $(3, 3) + S$. Will the coset $(4, 2) + S$ coincide with this line? (Use the previous result).
   4. In $\mathbf{Z}$, consider the subgroup $S = 4\mathbf{Z}$. Show that the cosets $(1 + 2) + S$ and $(5 + 6) + S$ are the same.

7. Let S be a subgroup of a group G. We will use the observations of the previous question to define addition of cosets. Let $a, b \in G$. Define the sum of cosets $a + S$ and $b + S$ as the coset $(a + b) + S$. Note that by the previous question, we have seen that if $a + S = x + S$ and $b + S = y + S$, then $(a + b) + S = (x + y) + S$. Thus, the sum is "well defined" in the sense that it is independent of the choice of the element used to define a coset. (Understand what is meant by this well definedness properly!). Show that with this definition, the set of cosets of S form a group. When $G = \mathbf{Z}$ and $S = 4\mathbf{Z}$, what is the inverse of the element $1 + S$? When $G = \mathbf{R}^2$ and S consists of all points in the line $x + y = 0$, what is the inverse of the coset defined by $x + y = 2$? □