MFCS Assignment I

1. Let G be an abelian group. Let $H \subseteq G$ be a subgroup of G. For $a \in G$ define the left coset of H defined by a $aH = \{ah : h \in H\}$. Define $G/H = \{aH : a \in G\}$. Note that each element in G/H is a set of the form aH. □

    1. Show that $a \in aH$.
    2. Suppose $a' \in aH$ then $aH = a'H$.
    3. Show that if $a' \in aH$, $b' \in bH$ then $a'b'H = abH$.
    4. Show that G/H with the multiplication defined by the above is an (abelian) group. This group is called the *Quotient Group* of G defined by H.
    5. Show that the function $f : G \to G/H$ defined by $f(a) = aH$ is a homomorphism from G to G/H.
    6. Consider $G = Z$, the set of integers with addition and $G' = Z_n$, the $\mod n$ system with addition. For natural number n, Let $nZ = \{in : i \in Z\}$. Show that nZ is a subgroup of Z. The quotient map Z/nZ is the same as (isomorphic to) G'..

2. Let G, G' be abelian groups. Let $f : G \to G'$ be a homomorphism from G to G'. (ie., the map f satisfies $f(g_1 + g_2) = f(g_1) + f(g_2)$ for all $g_1, g_2 \in G$.) Define $ker(f) = \{g \in G : f(g) = 0\}$ and $img(f) = \{g' \in G' : g' = f(g)$ for some $g \in G\}$. □

    1. Show that $ker(f)$ and $img(f)$ are subgroups of G and G' respectively.
    2. Show that the f is an injective if and only if $ker(f) = 0$ and f is surjective if and only if $img(f) = G'$.
    3. Let $H = kef(f)$. Consider the map $\overline{f} : G/H \to Img(f)$ defined by $\overline{f}(aH) = f(a)$. Show that the map is well defined. (ie. show that if $aH = a'H$ then $\overline{f}(aH) = f(a'H)$.)
    4. Show that $\overline{f}$ is a homomorphism which is both injective and surjective, hence an isomorphism. This result is called the *first homomorphism theorem* for groups.
    5. Define $f : Z \to Z_n$ be defined as $f(a) = amodn$. Show that f is a group homomorphism with respect to addition. What is $ker(f)$? Apply the homomorphism theorem for this map and draw your conclusion.

    The next two questions extend the above results to rings. Ring in this context means commutative ring with unity.

3. Let R be a (commutative) ring (with unity). Let $I \subseteq R$ be an *ideal* in R. For $a \in R$ define the left coset of I defined by a $a + I = \{a + i : i \in I\}$. Define $R/I = \{a + I : a \in R\}$. Note that each element in R/I is a set of the form $a + I$. □

    1. Show that $a \in a + I$.
    2. Suppose $a' \in a + I$ the $a + I = a' + I$.
    3. Show that if $a' \in a + I$, $b' \in b + I$ then $(a' + b') + I = (a + b) + I$ and $a'b' + I = ab + I$.
    4. Show that R/I with addition and multiplication that follows from the above problem a ring. This ring is called the *Quotient ring* of R defined by I.
    5. Show that the function $f : R \to R/I$ defined by $f(a) = a + I$ is a homomorphism from R to R/I.
    6. Consider $R = Z$, the set of integers with addition and multiplication, $R' = Z_n$, the $\mod n$ system with addition and multiplication. For natural number n, Let $nZ = \{in : i \in Z\}$. Show that nZ is an ideal in Z. Show that the quotient map Z/nZ is isomorphic to Z_n.

4. Let R, R' be rings. Let $f : R \to R'$ be a homomorphism from R to R'. Define $ker(f) = \{r \in R : f(r) = 0\}$ and $img(f) = \{r' \in R' : r' = f(r)$ for some $r \in R\}$. $\square$

    1. Show that $ker(f)$ is an ideal in R and $img(f)$ is a subring of R'.
    2. Show that the f is an injective if and only if $ker(f) = 0$ and f is surjective if and only if $img(f) = R'$.
    3. Let $I = kef(f)$. Consider the map $\overline{f} : R/I \to Img(f)$ defined by $\overline{f}(a + I) = f(a)$. Show that the map is well defined. (ie. show that if $a + I = a' + I$ then $\overline{f}(a + I) = f(a' + I)$.)
    4. Show that $\overline{f}$ is a homomorphism which is both injective and surjective, hence an isomorphism. This result is called the *first homomorphism theorem* for rings.
    5. Define $f : Z \to Z_n$ be defined as $f(a) = amodn$. Show that f is a ring homomorphism. What is $ker(f)$? Apply the homomorphism theorem for this map and draw your conclusion.
    6. Let F be a field and $F[x]$ the set of polynomials with coefficients in F. Let $g(x) \in F[x]$. Show that the multiples of $g(x)$ in $F[X]$ denoted by $g(x)F[x]$ is an ideal in $F[x]$. Note that the quotient ring $F[x]/g(x)F[x]$ is the modulo $g(x)$ system.