MATH 307 C.K. LI Sample Exam. I

1. Let H be the set of real matrices of the form $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ with $a, b \in \mathbb{R}$.

   (a) Show that $(\mathbb{C}, +)$ is isomorphic to $(H, +)$.

   (b) Show that $(\mathbb{C}, \cdot)$ is isomorphic to $(H, \cdot)$.

   Solution. Define $\phi : \mathbb{C} \to H$ by $\phi(a + ib) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

   Then $\phi(a + ib) = \phi(c + id)$ implies $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$. So $a + ib = c + id$.

   Clearly, for any $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ with $a, b \in \mathbb{R}$, we have $\phi(a + ib) = A$. Thus, ϕ is surjective.

   Now, for $z_1 = a + ib$ and $z_2 = c + id$, we have

$$\phi(z_1) + \phi(z_2) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} = \phi(z_1 + z_2)$$

   and

$$\phi(z_1)\phi(z_2) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(ac + bd) \\ ac + bd & ac - bd \end{pmatrix} = \phi(z_1 z_2).$$

2. Let S be the set of all injective functions $f : \mathbb{N} \to \mathbb{N}$. Under the operation of function composition, show that the group axioms (G0), (G1) and (G2) hold, but (G3) fails.

   Solution. (G0) Suppose $f, g : \mathbb{N} \to \mathbb{N}$ are one-one. If $f(g(x)) = f(g(y))$ then $g(x) = g(y)$. So $x = y$. Hence fg is one-one.

   (G1) Function composition is associative.

   (G2) The identity function $\phi(x) = x$ is one-one, and $\phi f = f = f\phi$ for all $f : \mathbb{N} \to \mathbb{N}$.

   (G3) may not hold. For example, if $f(x) = 2x$, then there is no $g : \mathbb{N} \to \mathbb{N}$ such that $fg = gf = \phi$.

3. Suppose G is a group. Show that $Z = \{x \in G : xg = gx \text{ for all } g \in G\}$ is a subgroup of G.

   Solution. Evidently, $eg = ge$ for all $g \in G$. So, $e \in Z$.

   If $x, y \in Z$, then $xg = gx$ and $yg = gy$ for all $g \in G$. Hence $(xy)g = xgy = g(xy)$ so that $xy \in Z$.

   If $x \in Z$, then $xg = gx$ for all $g \in G$ and thus

$$x^{-1}g = x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1} = gx^{-1}.$$

4. (a) Let g be an element of a finite group G. Show that $g^{-1} = g^k$ for some positive integer k.

   (b) Give an example of an infinite group H and $h \in H$ such that $h^{-1} \neq h^m$ for any positive integer m.

   Solution. Suppose G has n element. Then $g, g^2, \ldots, g^{n+1}$ cannot be all distinct. So, there is $1 \leq p < q \leq n + 1$ such that $g^p = g^q$. Hence $g^{q-p} = e$. If $q - p = 1$ then $g = e$ and $g^{-1} = g$. Otherwise, $k = q - p - 1 \geq 1$ and $g^k g = e = gg^k$ so that $g^{-1} = g^k$.

   (b) Consider 2 in the group $(\mathbb{R}^+, \cdot)$. Then $2^k \neq 2^{-1}$ for any positive integer k.

5. Suppose p and q are two distinct prime numbers.

   (a) Determine the number of generators of $\mathbb{Z}_{pq}$.

   (b) Determine the subgroup lattice diagram of $\mathbb{Z}_{pq}$.

   Solution. (a) Let $0 \leq r < pq$. Then $\gcd(r, pq) = 1$ if and only if

$$r \notin \{0\} \cup \{mp : 1 \leq m < q\} \cup \{mq : 1 \leq m < p\}.$$

   Thus, there are $pq - p - q + 1$ so many generators.

   (b) There are 4 subgroups, namely, $\mathbb{Z}_{pq} = \langle 1 \rangle$, $\langle p \rangle$, $\langle q \rangle$, and $\{0\}$. Clearly, $\langle p \rangle$ and $\langle q \rangle$ lie between $\mathbb{Z}_{pq}$ and $\{0\}$.

6. (a) Let $\tau = (3, 7, 2, 1)$. Show that $\sigma^{-1}\tau\sigma = (1, 2, 3, 4)$ if $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$.

   (b) For each k-cycle $\tau = (i_1, \ldots, i_k)$ in S_n, show that there is $\sigma \in S_n$ such that $\sigma^{-1}\tau\sigma = (1, 2, \ldots, k)$.

   Solution. (a) Consider the effect of $\sigma^{-1}\tau\sigma$ on $\{1, \ldots, 7\}$.

   $\sigma^{-1}\tau\sigma(1) = \sigma^{-1}\tau(3) = \sigma^{-1}(7) = 2$, $\sigma^{-1}\tau\sigma(2) = \sigma^{-1}\tau(7) = \sigma^{-1}(2) = 3$,

   $\sigma^{-1}\tau\sigma(3) = \sigma^{-1}\tau(2) = \sigma^{-1}(1) = 4$, $\sigma^{-1}\tau\sigma(4) = \sigma^{-1}\tau(1) = \sigma^{-1}(3) = 1$,

   $\sigma^{-1}\tau\sigma(5) = \sigma^{-1}\tau(5) = \sigma^{-1}(5) = 5$, $\sigma^{-1}\tau\sigma(6) = \sigma^{-1}\tau(6) = \sigma^{-1}(6) = 6$,

   $\sigma^{-1}\tau\sigma(7) = \sigma^{-1}\tau(4) = \sigma^{-1}(5) = 7$. Thus $\sigma^{-1}\tau\sigma = (1, 2, 3, 4)$.

   (b) Let

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & \cdots & n \\ i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_n \end{pmatrix},$$

   where $\{1, \ldots, n\} = \{i_1, \ldots, i_n\}$.

   If $1 \leq r < k$, then $\sigma^{-1}\tau\sigma(r) = \sigma^{-1}\tau(i_r) = \sigma^{-1}(i_{r+1}) = r + 1$.

   Also, $\sigma^{-1}\tau\sigma(k) = \sigma^{-1}\tau(i_k) = \sigma^{-1}(i_1) = 1$.

   If $r > k$, then $\sigma^{-1}\tau\sigma(r) = \sigma^{-1}\tau(i_r) = \sigma^{-1}(i_r) = r$.