Math 71 Midterm Solutions

1. $f, g, h \in M(S)$ let $s \in S$

$f(gh)(s) = f(gh(s)) = f(g(h(s)))$

$(fg)h(s) = (fg)(h(s)) = f(g(h(s)))$

They are equal $\therefore f(gh) = (fg)h$

Let e be the identity fcn $S \to S$

$(fe)(s) = f(e(s)) = f(s) \quad \therefore fe = f$

Sim. $ef = f \quad \therefore M(S)$ is a monoid

No. of element of $M(S) = n^n$

2. e identity, t switching $t(1) = 2$, $t(2) = 1$

f_1, $f_1(i) = 1$ .. $f_2(i) = 2$

	e	f_1	f_2	t
e	e	f_1	f_2	t
f_1	f_1	f_1	f_2	f_2
f_2	f_2	f_1	f_2	f_1
t	t	f_1	f_2	e

3. M finite monoid If $m \in M$ define $L_m : M \to M$ by

$L_m(x) = mx \quad \therefore L_m \in M(M)$

Define $\theta : M \to M(M)$ by $\theta(m) = L_m$

Show θ homomorphism of monoids: $\theta(mn) = L_{mn} = L_m L_n = \theta(m)\theta(n)$. Show θ one-one: Suppose $\theta(m) = \theta(m')$ $\therefore L_m = L_{m'}$ $\therefore m = L_m(e) = L_{m'}(e) = m'$ $\therefore \theta$ mono.

4. Show $a, a' \in U(M) \Rightarrow aa' \in U(M)$

$\exists\, b, b'$ $ab = e = ba$, $a'b' = e = b'a'$. Then

$(aa')(b'a') = aea' = e$ Similarly $(b'a')(aa') = e$.

$\therefore U(M)$ closed under mult. The operation in $U(M)$ is associative (since $U(M) \subseteq M$ and M is associative) $e \in U(M)$ since $ee = e$. Finally $a \in U(M) \Rightarrow \exists\, b$, $ab = ba = e$

$\therefore b \in U(M)$ and $b = a^{-1}$. $\therefore U(M)$ is a group.

II 1. Clearly $a \in Z(G) \Rightarrow as = sa \quad \forall s \in S$

Suppose now $as = sa \quad \forall s \in S$.

$\therefore \quad a = ass^{-1} = sas^{-1} \qquad \therefore s^{-1}a = s^{-1}sas^{-1} = as^{-1}$

$\therefore$ a commutes with s^{-1}! Given $x \in G$ then

$$x = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} \quad \text{where } s_i \in S \text{ and } \epsilon_i = \pm 1$$

$\therefore$ If a commutes with all $s \in S$

$$ax = a s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} a \quad \text{since } a \text{ commutes}$$
$$= xa \quad \text{with all } s_i^{\epsilon_i}$$

$\therefore$ a commutes with all $x \in G \quad \therefore a \in Z(G)$.

2. By 1., $a \in Z(D_{2n}) \Leftrightarrow ar = ra$ and $as = sa$

If ~~suppose~~ $a = sr^k$, then $ar = sr^{k+1}$ and $ra = rsr^k = sr^{-1}r^k = sr^{k-1} \quad \therefore sr^k \notin Z(D_{2n})$.

If $a = r^k \quad ar = ra$ and $as = r^k s = sr^{-k}$ and $sa = sr^k$. $\therefore r^k \in Z(D_{2n}) \Leftrightarrow r^{-k} = r^k \Leftrightarrow r^{2k} = 1$

$\Leftrightarrow 2k = n \quad \therefore Z(D_{2n}) = 1$ if n odd $\quad Z(D_{2n}) = \{1, r^k\}$ if n even $= 2k$.

3. Suppose a is the element of order 2 and $x \in G$ is any element then xax^{-1} is an element of order 2 (it is just conjugation of a by x and that is an isomorphism) or $(xax^{-1})(xax^{-1}) = xaeax^{-1} = xa^2x^{-1} = xex^{-1} = e$.

$\therefore xax^{-1} = a$ (by uniqueness) $\therefore xa = ax \quad \forall x \in G$

$\therefore a \in Z(G)$

4. Let $Z(G) = H$. Since G/H is cyclic $G/H = \langle aH \rangle$ for some $a \in G$. Let $x, y \in G$ then $xH = (aH)^n = a^n H$ and $yH = a^m H$ some m, n. $\therefore$ ~~[illegible]~~

$a^{-n}x \in H$, $a^{-m}y \in H$ (same coset property).

$\therefore\ a^{-n}x = z,\quad a^{-m}y = z'\quad$ some $z, z' \in H = Z(G)$

$\therefore\ x = a^n z,\ y = a^m z'$ Therefore

$xy = a^n z\, a^m z' = a^{n+m} z z'$ (since $z \in Z(G)$)

$yx = a^m z' a^n z = a^{m+n} z' z = a^{m+n} z z'$

$\therefore\ xy = yx$

III ~~Hallaw~~ The orbits partition A into disjoint subsets

$$A = \mathcal{O}(a_1) \cup \cdots \cup \mathcal{O}(a_k)$$

For any orbit $\mathcal{O}(a_i)$,

$|G/G_{a_i}| = |\mathcal{O}(a_i)|$ where G_{a_i} is the stability group of a_i.

$|G/G_{a_i}| = [G : G_{a_i}] \mid |G| = p^\alpha \quad \alpha \geq 1$

$\therefore\ |G/G_{a_i}| = p^{b_i},\quad 0 \leq b_i$

Every orbit has order a power of p, ie.

$$|\mathcal{O}(a_i)| = p^{b_i},\quad b_i \geq 0$$

If all orbits have order p^{b_i} with $b_i > 0$ then

$|A| = p^{b_1} + p^{b_2} + \cdots + p^{b_k}$ which is divisible by p.

Impossible. Therefore for some i, $b_i = 0$ and so

$G = G_{a_i}\quad \therefore\ \forall g \in G\quad g a_i = a_i$ so a_i is a fixed point.