NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Lin Mingyan Simon, Chang Hai Bin

MA2202 Algebra I
AY 2009/2010 Sem 2

Question 1

(a) By expressing g as a product of disjoint cycles, we see that $g = (1\,2)(1\,2\,3)(1\,2\,3\,4\,5) = (1\,3\,4\,5)$. So $o(g) = 4$ and hence $g^{222} = (g^4)^{55}g^2 = [(1)]^{55}(1\,3\,4\,5)(1\,3\,4\,5) = (1\,4)(3\,5)$.

(b) We note that the alternating group A_4 consists of the even permutations of the set $\{1, 2, 3, 4\}$, namely the identity, the double transpositions and the 3-cycles of S_4. It is easy to see that the elements of T must have either order 1 or order 2, so this implies that $T = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. This implies that T is a Klein four-group, which is a subgroup of A_4.

Question 2

(a) (i) Note that $o([1]_{11}) = 11$, $o([1]_{17}) = 17$ and $(11, 17) = 1$. Therefore, we have $o(g) = o(([1]_{11}), ([1]_{17})) = \operatorname{lcm}(o([1]_{11}), o([1]_{17})) = 11 \cdot 17 = 187$.

(ii) Since $|\langle g\rangle| = o(g) = 187 = 11 \cdot 17 = |G_1| \cdot |G_2| = |G|$, it follows that $G = \langle g\rangle$ (which is cyclic).

(iii) Let the set of generators of G be A and $B = \{([a]_{11}, [b]_{17}) | a, b \in \mathbb{Z}, 0 < a < 11, 0 < b < 17\}$. We shall show that $A = B$.
Note that g_i is a generator of G if and only if $o(g_i) = 187$. Based on this fact, by a similar argument as in part (i) we can show that $A \supseteq B$. Conversely, take any generator $g_i = ([a]_{11}, [b]_{17})$. Then $o(([a]_{11}), ([b]_{17})) = \operatorname{lcm}(o([a]_{11}), o([b]_{17})) = 187 = 11 \cdot 17$. This can only happen if and only if $(a, 11) = 1$ and $(b, 17) = 1$. So we have $A \subseteq B$. Hence the desired holds.

(b) (i) Take any $h = (([a]_3), ([b]_6)) \in H$. Then the possible values of $o([a]_3)$ are 1 and 3, and the possible values of $o([b]_6)$ are $1, 2, 3$ and 6. As $o(h) = o(([a]_3), ([b]_6)) = \operatorname{lcm}(o([a]_3), o([b]_6))$, it follows that the possible values of $o(h)$ are $1, 2, 3$ and 6. Hence $\{o(h) |\, h \in H\} = \{1, 2, 3, 6\}$ and thus $\operatorname{lcm}\{o(h) |\, h \in H\} = 6$.

(ii) Since $o(h) < 18 = 3 \cdot 6 = |H_1| \cdot |H_2| = |H|$ for all $h \in H$, we conclude that H is not cyclic.

Question 3

(i) We have $\tau(a_1\,a_2\,a_3)\tau^{-1} = (\tau(a_1)\,\tau(a_2)\,\tau(a_3)) = (a_2\,a_1\,a_4)$. Hence, a possible mapping for τ is $\tau(a_1) = a_2$, $\tau(a_2) = a_1$, $\tau(a_3) = a_4$ and $\tau(a_4) = a_3$, so one has $\tau = (a_1\,a_2)(a_3\,a_4)$. This implies that $\tau \in A_4$ so we are done.

(ii) Since $|A_4 : H| = \frac{|A_4|}{|H|} = \frac{12}{6} = 2$ by Lagrange's Theorem, H has an index of 2 in A_4 and therefore H is a normal subgroup of A_4.

(iii) Suppose such a subgroup H of A_4 with order 6 exists. Then H is necessarily normal and H must contain a 3-cycle $(a_1\,a_2\,a_3)$. WLOG, we shall assume that $\min\{a_1, a_2, a_3\} = a_1$.

If $(a_1\,a_2\,a_3) = (1\,3\,2)$, then we see that $(1\,2\,3) = (1\,3\,2)^{-1} \in H$. Also, by the normality of H, we must have $(2\,4\,3)(1\,3\,2)(2\,4\,3)^{-1} = (1\,2\,4) \in H$. Therefore, one has $A_4 = \langle(1\,2\,3), (1\,2\,4)\rangle \subseteq H \subseteq A_4$, giving us $H = A_4$, which is not of order 12, a contradiction.
If $(a_1\,a_2\,a_3) = (1\,4\,2)$, then we see that $(1\,2\,4) = (1\,4\,2)^{-1} \in H$. Also, we must have $(2\,3\,4)(1\,4\,2)(2\,3\,4)^{-1} = (1\,2\,3) \in H$. Then by a similar argument above, we would arrive at the same contradiction.
If $(a_1\,a_2\,a_3) = (1\,4\,3)$, then we see that $(2\,4\,3)(1\,4\,3)(2\,4\,3)^{-1} = (1\,3\,2) \in H$. This reduces to our first case above.
If $(a_1\,a_2\,a_3) = (2\,4\,3)$, then we see that $(1\,3\,2)(2\,4\,3)(1\,3\,2)^{-1} = (1\,4\,2) \in H$. This reduces to our second case above.

Finally, if $(a_1\,a_2\,a_3) = (1\,2\,3)$, $(1\,2\,4)$, $(1\,3\,4)$ or $(2\,3\,4)$, then by using the fact that H is closed under inversion, we may reduce it to one of the four cases above.
So no such H exists, and hence we conclude that A_4 contains no subgroup of order 6.

Question 4

(i) Let the other non-identity element of G be g_3. Then define the function $f : (U(\mathbb{Z}/(8)), \times) \to G$ as follows: $f(\bar{1}) = e_G$, $f(\bar{3}) = g_1$, $f(\bar{5}) = g_2$, $f(\bar{7}) = g_3$. Then it is easy to see that f is a bijection satisfying the conditions.

(ii) As f is already a bijection, it only suffices to check that f is a homomorphism. By direct computation it is easy to check that $g_1g_2 = g_3 = g_2g_1$, $g_1g_3 = g_2 = g_3g_1$ and $g_2g_3 = g_1 = g_3g_2$.

Now, take any two elements $a, b \in (U(\mathbb{Z}/(8)), \times)$. We see that the equation $f(a\times b) = f(a)f(b)$ clearly holds when $a = \bar{1}$ or $b = \bar{1}$. Also, by observing that $\bar{3} \times \bar{3} = \bar{5} \times \bar{5} = \bar{7} \times \bar{7} = \bar{1}$, we see that the equation also holds when $a = b$ and a is a non-identity element.

Finally, by observing that $\bar{3} \times \bar{5} = \bar{7} = \bar{5} \times \bar{3}$, $\bar{3} \times \bar{7} = \bar{5} = \bar{7} \times \bar{3}$ and $\bar{5} \times \bar{7} = \bar{3} = \bar{7} \times \bar{5}$ and the above equations in G, we see that the equation also holds when both a and b are non-identity elements and $a \neq b$. So f is a homomorphism and hence an isomorphism.

(iii) Since $|G| = 4$, it follows that for any $g \in G$, we must have $o(g) = 1$, 2 or 4. If there exists some $g \in G$ such that $o(g) = 4$, then G is a cyclic group of order 4 and hence must be isomorphic to $(\mathbb{Z}/(4), +)$. Otherwise, we must have $o(g) \leq 2$ for all $g \in G$, which would imply that $g^2 = e_G$ for all $g \in G$. In this case, G must be isomorphic to $(U(\mathbb{Z}/(8)), \times)$. We are done.

Question 5

(i) We have $\tau_1(a_1\,a_2)\tau_1^{-1} = (\tau_1(a_1)\,\tau_1(a_2)) = (a_3\,a_4)$. Hence, a possible mapping for τ_1 is $\tau_1(a_1) = a_3$, $\tau_1(a_2) = a_4$, $\tau_1(a_3) = a_1$ and $\tau_1(a_4) = a_2$, so one has $\tau_1 = (a_1\,a_3)(a_2\,a_4)$.

We have $\tau_2(a_1\,a_2)(a_3\,a_4)\tau_2^{-1} = (\tau_2(a_1)\,\tau_2(a_2))(\tau_2(a_3)\,\tau_2(a_4)) = (a_1\,a_3)(a_2\,a_4)$. Hence, a mapping for τ_2 is $\tau_2(a_1) = a_1$, $\tau_2(a_2) = a_3$, $\tau_2(a_3) = a_2$ and $\tau_2(a_4) = a_4$, so one has $\tau_2 = (a_2\,a_3)$.

We have $\tau_3(a_1\,a_2\,a_3)\tau_3^{-1} = (\tau_3(a_1)\,\tau_3(a_2)\,\tau_3(a_3)) = (a_2\,a_3\,a_4)$. Hence, a possible mapping for τ_3 is $\tau_3(a_1) = a_2$, $\tau_3(a_2) = a_3$, $\tau_3(a_3) = a_4$ and $\tau_3(a_4) = a_1$, so one has $\tau = (a_1\,a_2\,a_3\,a_4)$.

(ii) Clearly, we have $\{(1)\} \subseteq Z(S_4)$. Pick any element $\sigma \in Z(S_4)$. Then we have $\sigma\tau = \tau\sigma$ for all $\tau \in S_4$, or equivalently, $\tau = \sigma\tau\sigma^{-1}$. This implies that $(1\,2) = \sigma(1\,2)\sigma^{-1} = (\sigma(1)\,\sigma(2))$ and $(1\,3) = \sigma(1\,3)\sigma^{-1} = (\sigma(1)\,\sigma(3))$. From the first equation we deduce that $\sigma(1) = 1$ and $\sigma(2) = 2$, or $\sigma(1) = 2$ and $\sigma(2) = 1$. If the latter holds, then we would have $(\sigma(1)\,\sigma(3)) = (2\,\sigma(3)) \neq (1\,3)$, which is a contradiction. So we must have $\sigma(1) = 1$ and $\sigma(2) = 2$, and thus from the second equation, we deduce that $\sigma(3) = 3$ and $\sigma(4) = 4$. Hence we have $\sigma = (1)$ and therefore $Z(S_4) \subseteq \{(1)\}$. We are done.

Question 6

(i) Let $\sigma, \tau \in H$. Then we must have $\sigma, \tau \in G$ so one has $\sigma\tau^{-1} \in G$, since G is a subgroup of S_n. Also, we have $\tau^{-1}(1) = \tau^{-1}(\tau(1)) = (\tau^{-1}\tau)(1) = 1$, so one has $(\sigma\tau^{-1})(1) = \sigma(\tau^{-1}(1)) = \sigma(1) = 1$. Hence, $\sigma\tau^{-1} \in H$ so H is a subgroup of G.

(ii) Define O_1 to be the orbit of $1 \in \{1, \cdots, n\}$, and define S_1 to be the stabilizer of $1 \in \{1, \cdots, n\}$. Since G acts transitively on the set $\{1, \cdots, n\}$ it follows that $|O_1| = n$. Also, it is easy to see that the stabilizer of $1 \in \{1, \cdots, n\}$ is precisely H. Therefore, by the Orbit-Stabilizer Theorem, we have $|G| = |O_1||S_1| = n|H|$ as desired.

Question 7

(i) Note that for any $g \in G$, one has $o(gH) \,|\, |G/H|$ by the Lagrange's Theorem. Therefore, one has $g^{|G/H|}H = (gH)^{|G/H|} = e_{G/H} = H$. This implies that $g^{|G/H|} \in H$ so we are done.

(ii) Let N be a subgroup of G of order H, i.e. $|N| = |H|$. Since $(|H|, |G/H|) = 1$, it follows that there exist $a, b \in \mathbb{Z}$, such that $a|H| + b|G/H| = 1$.
Hence, for all $x \in N$, we have $x = x^{a|H|+b|G/H|} = \left(x^{|N|}\right)^a \left(x^{|G/H|}\right)^b = \left(x^{|G/H|}\right)^b$ (since $x^{|N|} = e_G$). By part (i), we have $x^{|G/H|} \in H$, so $x \in H$. Therefore, $N \subseteq H$ so we must have $N = H$. This shows that H is the unique subgroup of G with order $|H|$ so we are done.

Question 8

(i) False. Let $G = A_4$ and $d = 6$. Then we see that $d = 6|12 = |A_4| = |G|$, but by Question 3, there exists no subgroup H of G whose order is equal to d.

(ii) False. Let $G = S_3$ and $p = 2$. Then we see that $|G| = |S_3| = 6$, so p is a prime divisor of $|G|$. However, $\{(1), (1\,2)\}$ and $\{(1), (1\,3)\}$ are distinct subgroups of G having order equal to p.

(iii) True. Let g_1 be a non-identity element of G_1, and let $g_2 = f(g_1)$. Note that $o(g_1)||G_1| = 10$ and $o(g_2)||G_2| = 21$. Then one has $g_2^{o(g_1)} = [f(g_1)]^{o(g_1)} = f\left(g_1^{o(g_1)}\right) = f(e_{G_1}) = e_{G_2}$, so this implies that $o(g_2)|\,o(g_1)|10$. As $(10, 21) = 1$ and $o(g_2)$ divides both 10 and 21 it follows that $o(g_2) = 1$. So $g_2 = e_{G_2}$ and hence $f(G_1) = \{e_{G_2}\}$.

(iv) True. If $G = \langle g \rangle$ has infinite order, then the map $\psi : (\mathbb{Z}, +) \to G$, $\psi(n) = g^n$ is clearly an isomorphism (and is hence surjective). Otherwise, if $o(g) = m < \infty$, then the map $\phi : (\mathbb{Z}/(m), +) \to G$, $\phi(\bar{n}) = g^n$, is an isomorphism (and is hence surjective). As the canonical projection homomorphism $\pi : (\mathbb{Z}, +) \to (\mathbb{Z}/(m), +)$ is clearly surjective, we see that the homomorphism $\psi = \phi \circ \pi : (\mathbb{Z}, +) \to G$ is surjective. We are done.

(v) False. Take $G = S_3$ and $H = \langle (1\,2\,3) \rangle$, $g = (1\,2)$ and $h = (1\,2\,3) \in H$. Since $|H| = 3$, we see that $|G : H| = \frac{|G|}{|H|} = \frac{6}{3} = 2$. This implies that H has an index of 2 in G so H is necessarily normal in G. However, we have $h = (1\,2\,3) \neq (1\,3\,2) = (1\,2)(1\,2\,3)(1\,2) = ghg^{-1}$.

(vi) True. Since N_1 and N_2 are normal in G it follows that $gn_1g^{-1} \in N_1$ and $gn_2g^{-1} \in N_2$ for all $n_1 \in N_1$, $n_2 \in N_2$ and $g \in G$. Now, take $h \in N_1N_2$. Then $h = h_1h_2$ for some $h_1 \in N_1$ and $h_2 \in N_2$ so this implies that $ghg^{-1} = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) \in N_1N_2$. So N_1N_2 is normal in G.

(vii) False. Take $G = S_3$ and $N = \langle (1\,2\,3) \rangle$. Since N is cyclic, N is necessarily abelian. Also, by part (v) we have shown that $|G/N| = |G : N| = 2$, so this implies that G/N has a prime order. Hence it is necessarily cyclic (and thus abelian). However, G is not abelian.

(viii) True. Take $h, k \in T_n(G)$. Then one has $h^n = k^n = e_G$. Now we have

$$\begin{aligned}
\left(hk^{-1}\right)^n &= \underbrace{\left(hk^{-1}\right)\left(hk^{-1}\right)\cdots\left(hk^{-1}\right)}_{n\text{ times}} \\
&= \underbrace{hh\cdots h}_{n\text{ times}}\underbrace{k^{-1}k^{-1}\cdots k^{-1}}_{n\text{ times}} \quad \text{(because } G \text{ is abelian)} \\
&= h^n\left(k^{-1}\right)^n \\
&= e_G\left(k^n\right)^{-1} \\
&= e_G^{-1} = e_G.
\end{aligned}$$

This implies that $hk^{-1} \in T_n(G)$ so $T_n(G)$ is a subgroup of G.