NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to He Jinxin

MA2202 Algebra I
AY 2007/2008 Sem 2

Question 1

(a) Firstly, note that since $Z/(19^2) \times Z/(17^2)$ is cyclic, it has unique subgroups of each order dividing $17^2 \times 19^2$.
Let H be a subgroup of $Z/(17^2) \times Z/(19^2)$, Hence $|H| = 1$ or 17 or 19 or 17^2 or 19^2 or 17×19 or 17×19^2 or $17^2 \times 19$ or $17^2 \times 19^2$.
So the subgroups of $Z/(17^2) \times Z/(19^2)$ are:
$\{0\} \times \{0\}$,
$H_{17} \times \{0\}$, $\{0\} \times H_{19}$,
$H_{17} \times H_{19}$, $Z/(17^2) \times \{0\}$, $\{0\} \times Z/(19^2)$,
$Z/(17^2) \times H_{19}$, $H_{17} \times Z/(19^2)$ and
$Z/(17^2) \times Z/(19^2)$.

(b) Let $a, b \in Z/(3)$ such that $Z/(3) \times Z/(3) = \langle a \rangle \times \langle b \rangle$. Then the subgroups of $Z/(3) \times Z/(3)$ are
$\{0\} \times \{0\}$,
$\langle a \rangle \times \{0\}$, $\{0\} \times \langle b \rangle$, $\langle (a, b) \rangle$,$\langle (2a, b) \rangle$,
$\langle a \rangle \times \langle b \rangle$.

Question 2

(i) Let the order of g^{14} be n, then $(g^{14})^n = 1$. Hence $14n \equiv 0 \mod 30$, which means $14n = 30k$ for some integer k. So $7n = 15k$, since $3 \mid 15k$ and $5 \mid 15k$ but $3 \nmid 7$ and $5 \nmid 7$, we have $15 \mid n$. Then since $(g^{14})^{15} = g^{210} = (g^{30})^7 = 1$, we have $n \mid 15$. Hence we have $n = 15$. i.e. $o(g^{14}) = 15$.

(ii) $\forall$ m such that $o(g^m) = o(g^{14}) = 15$, then $(g^m)^{15} = 1$ and $(g^m)^k \neq 1$ for $k = 1, 2, ...14$.
So we have $15m \equiv 0 \mod 30$, then $m \equiv 0 \mod 2$, we set $m = 2l$.
And $km \not\equiv 0 \mod 30$, then $2lk \not\equiv 0 \mod 30$, $lk \not\equiv 0 \mod 15$ for all $k = 1, 2, ..., 14$. Therefore, l is not divisible by 3 and 5.
Hence $l = 1$ or 2 or 4 or 6 or 7 or 8 or 11 or 13 or 14. Hence the set of elements of G whose order is equal to $o(g^{14})$ is $\{2, 4, 8, 14, 16, 22, 26, 28\}$.

Alternative solution:
Since $\langle g \rangle$ is cyclic it has exactly 1 subgroup of order 15. Hence all elements of order 15 in $\langle g \rangle$ lie in this subgroup and are exactly the generator of this subgroup. Hence there are $\phi(15) = 8$ such element. Let $h = g^{14}$ then $\langle h \rangle$ is the unique subgroup of order 15 and the generators of this subgroup are precisely elements of the form h^m such that $m \in \{0, ..., 14\}$ and $\gcd(m, 15) = 1$. Hence set of elements of order 15 is $\{(g^{14})^m \mid \gcd(m, 15) = 1 \text{ and } m \in \{0, 1, ..., 14\}\}$.

Question 3

(a) Since $\langle(12)(34),(13)(24)\rangle = \{1,(12)(34),(13)(24),(14)(23)\}$ is the subgroup of **all** $2,2$ cycles and conjugation preserves cycle structure. $\langle(12)(34),(13)(24)\rangle \lhd S_4$.

(b) No.$(15)(12)(34)(15) = (15)(34) \notin \langle(12)(34),(13)(24)\rangle$.

(c) *Claim: For any $\sigma \in S_3V$ there exist unique $p \in S_3$,$q \in V$ such that $pq = \sigma$.*
Proof:
Existence:
Since $S_3 \subseteq S_4$, for every $\alpha \in V$ we have $\alpha S_3 = S_3\alpha$. Therefore we have $S_3V = VS_3$ as groups.
Hence for all $\sigma \in S_3V$ there exist a finite sequence of $p_1p_2, p_3, ..., p_n \in S_3$ and $q_1, q_2, q_3, ..., q_n \in V$ such that $p_1q_1p_2q_2...p_nq_n = \sigma$.
Since $S_3V = VS_3$ for each p_i, q_j such that $i, j \in \{1, 2, ..., n\}$. There exists $p'_i \in S_3$ and $q'_j \in V$ such that $p_iq_j = q'_jp'_i$.
Therefore we may rearrange and rewrite $p_1q_1p_2q_2...p_nq_n$ to $p'_1p'_2...p'_nq'_1q'_2...q'_n$ such that $p'_i \in S_3$ and $q'_j \in V$ with $i, j \in \{1, 2, ..., n\}$ and $\sigma = p_1q_1p_2q_2...p_nq_n = (p'_1p'_2...p'_n)(q'_1q'_2...q'_n)$.

Uniqueness:
Suppose $p, p' \in S_3$ and $q, q' \in V$ such that $pq = p'q'$. Hence we have $p'^{-1}p = q'q^{-1}$. Hence $q'q^{-1} \in S_3 \cap V$. Hence we have $q'q^{-1}(4) = 4$ and $q'q^{-1} = (1)$. Therefore $q = q'$ and $p = p'$. □

Hence we may define the map

$$\begin{aligned} f : S_3V &\rightarrow S_3 \\ pq &\mapsto p \end{aligned}$$

where $p \in S_3$, $q \in V$ such that $pq = \sigma$ is the unique decomposition of σ.This is a well defined function by the previous claim.

Claim:This map is a well-defined homomorphism.
Proof:
For any $p_1q_1, p_2q_2 \in S_3V$, we have

$$\begin{aligned} f(p_1q_1p_2q_2) &= f\left(p_1p_2(p_2^{-1}q_1p_2)q_2\right) \\ &= p_1p_2 \qquad\qquad \text{since } V \lhd S_3V \\ &= = f(p_1q_1)f(p_2q_2) \end{aligned}$$

□

Also, since f is surjective and $\ker(f) = V$. By First Isomorphism Theorem, we have $S_3 \cong S_3V/V$.

(d) Since $S_3 \cong S_3V/V$, we have $|S_3||V| = |S_3V|$. Hence $|S_3V| = 24$. Since $S_3V \subseteq S_4$ and $|S_3V| = |S_4|$, we have $S_3V = S_4$. □

Question 4

(a) For all $A \in C_G(P)$, let $A = \begin{pmatrix} d & e \\ f & g \end{pmatrix}$
. If $AP = PA$, then

$$\begin{pmatrix} d & e \\ f & g \end{pmatrix} \begin{pmatrix} \epsilon & 0 \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} \epsilon & 0 \\ 0 & \delta \end{pmatrix} \begin{pmatrix} d & e \\ f & g \end{pmatrix}$$

Hence we have,

$$\begin{aligned} e\delta &= \epsilon e \\ f\epsilon &= \delta f \\ \epsilon &\neq \delta \end{aligned}$$

which derives $e = f = 0$.
Then $C_G(P) = D_2(R) = \left\{ \begin{pmatrix} d & 0 \\ 0 & g \end{pmatrix} |d, g \in R \right\}$.

(b) Obviously $Z(G) \supset C_G(P)$. That is the center $Z(G)$ has the form

$$\begin{pmatrix} d & 0 \\ 0 & g \end{pmatrix}$$

.
If $d \neq g$, then

$$\begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & g \end{pmatrix} \neq \begin{pmatrix} d & 0 \\ 0 & g \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix}$$

.
If $d = g$,we have

$$\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ w & z \end{pmatrix} = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} dx & dy \\ dw & dz \end{pmatrix}$$

for all $\begin{pmatrix} x & y \\ w & z \end{pmatrix} \in G$.
Therefore

$$Z(G) = \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} |r \neq 0 \in R \right\}$$

.

Question 5

(a) (i) Because G_2 is abelian, then for all $g, g' \in G_1$

$$\begin{aligned} f((g^{-1}g'^{-1}gg')) &= (f(g^{-1})f(g'^{-1})f(g)f(g')) \\ &= (f(g^{-1})f(g')f(g'^{-1})f(g)) \\ &= (f(g^{-1}g)f(g'^{-1}g')) = 1 \end{aligned}$$

.
Therefore $[g, g'] \in \ker(f)$ for all $g, g' \in G_1$. Since $[G_1, G_1]$ is generated by $\{[g, g']|g, g' \in G_1\}$, hence we have $[G_1, G_1] \subset \ker(f)$.

(ii) If $[G_i, G_i{}']\subset \ker(f)$, since f is surjective, for any $b_1, b_2 \in G_2$, there exists g_1, g_2 such that

$f(g_1) = b_1,\ f(g_2) = b_2$.
Then

$$\begin{aligned} 1 &= f(g_1^{-1} g_1 g_2^{-1} g_2) \\ &= f(g_1^{-1}) f(g_1) f(g_2^{-1}) f(g_2) \\ &= (f(g_2) f(g_1))^{-1} f(g_1) f(g_2) \end{aligned}$$

.
Hence $f(g_1)f(g_2) = f(g_2)f(g_1)$. Then $b_1 b_2 = b_2 b_1$, i.e. G_2 is abelian. □

(b) Let $\phi_{N_1} : G \to G/N_1$ and $\phi_{N_2} : G \to G/N_2$ be the canonical quotient maps,hence $\ker(\phi_{N_1}) = N_1$ and $\ker(\phi_{N_2}) = N_2$. They are both surjective and since both G/N_1 and G/N_2 are abelian, by 5(i) we have $[G, G] \le N_1$ and $[G, G] \le N_2$. Hence we have $[G, G] \le N_1 \cap N_2$.
Since $N_1 \lhd G$ and $N_2 \lhd G$, we have $N_1 \cap N_2 \lhd G$.
Let $\phi_{N_1 \cap N_2} : G \to G/N_1 \cap N_2$ be the canonical quotient map, hence $\ker(\phi_{N_1 \cap N_2}) = N_1 \cap N_2$.
Since $[G, G] \le N_1 \cap N_2$, by 5(ii) we have $G/N_1 \cap N_2$ is abelian.

Question 6

(a) Since $|G| = 6$, let $g \in G \backslash \{1\}$. Then order of g divides 6. Hence $o(g) =$ 2,3 or 6.
Also, note that any group of order 3 must be cyclic since 3 is prime.
If G only has elements of order dividing 2 then for all $g \in G$, $g = g^{-1}$. Hence $g_1 g_2 = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} = g_2 g_1$. Then G is abelian and any subgroup is normal. Hence $|G/\langle g\rangle| = 3$ for any $g \in G\backslash\{1\}$. Hence $G/\langle g\rangle$ is generated by $h\langle g\rangle$ for some $h \notin \langle g\rangle$.
Hence we have $h^3 \in \langle g\rangle$ but $h^3 = h \in \langle g\rangle$ which is a contradiction !!
Hence G must contain elements of order 3 or 6.
If $o(g) = 6$, then $G \cong \mathbb{Z}_6$. Hence $\{0, 2, 4\}$ would be a cyclic normal subgroup of order 3 since $\mathbb{Z}_6$ is abelian.
If $o(g) = 3$, then $\langle g\rangle$ is a cyclic normal subgroup of order 3 since it is of index 2.

(b) $< h > \lhd G$, then $g < h > g^{-1} =< h >$ for any $g \in G$. Hence $< ghg^{-1} >=< H >$.

(c) Since G contains a normal subgroup H of order 3. Hence $|G/H| = 2$. Therefore $G/H = \langle aH\rangle$ for some $a \notin H$ and $a^2 \in H$.
Let $H = \langle b\rangle$. Hence $a^2 = b^k$ where $k \in \{0, 1, 2\}$.

Case 1) $k = 1$ or 2.
Then $a^2 \ne 1$ and $o(a^2) = 3$ since $a^2 \in \langle b\rangle$. Hence $a^6 = 1$ and $a^2 \ne 1$. If $a^3 = 1$ then we have $a \in H$ since $ab^k = 1$ which is a contradiction!!
Since $o(a)|6$ and $a^2 \ne 1$ and $a^3 \ne 1$,we have $o(a) = 6$. Hence $G = \langle a\rangle \cong Z/(6)$.

Case 2) $k = 0$.
Then $a^2 = 1$ and $b^3 = 1$ and there exist a $m \in \{0, 1, 2\}$ such that

$$\begin{aligned} aba^{-1} &= b^m \\ a^2ba^{-2} &= ab^m a^{-1} \\ b &= ab^m a^{-1} \\ b &= (aba^{-1})^m \end{aligned}$$

Hence we have $(b^m)^m = b$ hence $3|m^2 - 1$. Hence $m = 1$or 2. If $m = 1$ then $ab = ba$. Then $o(ab) = \text{lcm}(o(a), o(b)) = 6$ and $G = \langle ab \rangle \cong Z/(6)$.
If $m = 2$ then we have $aba^{-1} = b^{-1}$ and $a^2 = 1$ and $b^3 = 1$ which are the defining conditions for $D_6 \cong S_3$. Hence $G \cong S_3$.

Question 7

(a) For any $r \in H$ since $r \neq 0$ $\frac{1}{r}$ is well-defined, $r \cdot \frac{1}{r} = 1$, $r \cdot 1 = 1$.
For any $r_1, r_2 \in H, r_1 \cdot r_2 \in H$ since the product of positive real numbers is positive. Therefore $H \leq G$.

(b) Consider the homomorphism $f : G \to \{1, -1\}$ with

$$f(r) = \begin{cases} 1 & \text{if } r > 0 \\ -1 & \text{if } r < 0 \end{cases}$$

.
Then we conclude that $ker(f) = H$, so $G/H \simeq \{1, -1\}$. So $[G : H] = 2$.

(c) φ is surjective.
Since $\forall y \in H$,from Real Analysis we know that there exist a positive real solution x to the equation $x^m - y = 0$. Hence $\varphi(x) = x^m = y$.

(d) Since G is abelian, any subgroup of normal. Hence let K be a subgroup of finite index in G. Then $H \cap K$ is also of finite index in G since $[G : H \cap K] = [G : H][H : H \cap K] = [G : H][G : K]$. In particular we have $[H : H \cap K] = m < \infty$ where $m \in \mathbb{N}$. Hence consider the homomorphism

$$\begin{aligned} \phi : H/H \cap K &\to H/H \cap K \\ hH \cap K &\mapsto (hH \cap K)^m = h^m H \cap K \end{aligned}$$

Note that since $m = |H/H \cap K|$. This is the trivial map(i.e $\text{Im}(\phi) = \{1\}$. But from part (c), this map is surjective. Hence $|H/H \cap K| = 1$. Therefore we have $H \cap K = H$. Hence $H = K$ or there exist $a \in K$ such that $a \notin H$. Hence $G = aH \cup H \subset K$. Therefore either $H = K$ or $G = K$.

$\square$

Question 8

(a) True.
$(g_1 * g_2) * g_3 = 1$, then $g_1 * (g_2 * g_3) = 1 \Rightarrow (g_2 * g_3)^{-1} = g_1 \Rightarrow (g_2 * g_3) * g_1 = 1$.

(b) False.
(1) is not in T.

(c) False. $Z/(2) \times Z/(4)$ is not cyclic even though $Z/(2)$ and $Z/(4)$ are both cyclic.

(d) False. Consider (12) and (123). Then $o((12)) = 2$ and $o((123)) = 3$ and $o((12)(123)) = o((23)) = 2 \neq \text{lcm}(2, 3)$.

(e) True.
We only need to show that for any $h \in H$,$h^{-1} \in H$.
For $h \in H$, $\exists i$ such that ${h_1}^i = 1$.
Otherwise $|H| = \infty$. Since $h^{i-1} = h^{-1}$ since $h^{i-1}h = 1$, we have $h^{-1} = h^{i-1} \in H$.

(f) True.
$ker(f) = \{1\}$, so f is injective hence $|G_1| \leq \mathrm{Im}(f)$ and since $|G_1| = |G_2| < \infty$, $\mathrm{Im}(f) \geq G_2$. Hence f is surjective and hence an isomorphism.

(g) False.
$o(A_5) = 60$ but A_5 doesn't have subgroup of order 30 since A_5 is simple.
Or $G = Z/(2) \times Z/(2)$, so $|G| = 4$ but G has no elements of order 4 since G is not cyclic.

(h) False.
$N \lhd G \Rightarrow \forall g \in G$, gN=Ng, but not necessarily $gn = ng$ $\forall n \in N$. An example would be $G = S_3$ and $N = A_3$. Hence $(12)(123) = (32) \neq (13) = (123)(12)$

(i) True.
We have $H_1 \cap H_2 \leq H_1$ and $H_1 \cap H_2 \leq H_2$. Hence $|H_1 \cap H_2|$ divides $\gcd(|H_1|, |H_2|) = 1$. Hence $|H_1 \cap H_2| = 1$. Therefore $|H_1H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = |H_1| \times |H_2|$.

(j) True.
Since $N_1, N_2 \lhd G$ we have $N_1N_2 \leq G$.
Hence for any $g \in G$. we have $gN_1N_2 = (gN_1)N_2 = (N_1g)(N_2) = N_1(gN_2) = N_1(N_2g) = N_1N_2g$.
Since $gN_1N_2 = N_1N_2g$ we have $N_1N_2 \lhd G$.