MA2202 - Algebra I Suggested Solutions

(Semester 1 : AY2019/20)

Written by : Jonathan Yeo
Audited by : Pan Jing Bin

Q1

(i)

If $gcd(m,n) = 1$, by Bezout's identity, $1 = am + bn$ for some $a, b \in \mathbb{Z}$.
Multiplying by N gives $amN + bnN = N$ and since $m|N$ and $n|N$ then we will have that $mn|amN$ and $mn|bnN$ and so $N = amN + bnN = kmn$ for some $k \in \mathbb{Z}$ and is a multiple of mn.

(ii)

Assume that $\gcd(m^2, n^3) = d > 1$ and that $p|d$ for some prime p. Then $p|m^2$ and $p|n^3$, and since p is prime, we have $p|m$ and $p|n$ thus $p|\gcd(m,n)$. But it is given that $\gcd(m,n) = 1$ so $p|1$ which is impossible so we conclude that $\gcd(m^2, n^3) = 1$.

Q2

(i)

($\Rightarrow$) If $m - n$ is a multiple of d then we will have $g^{m-n} = g^{qd} = (g^d)^q = e^q = e$. Thus $g^m = g^n$.
($\Leftarrow$) $g^m = g^n \implies g^{m-n} = e$. By the Euclidean Algorithm, $m - n = qd + r$ where $0 \leq r < d$, and we have $g^{m-n} = g^{qd+r} = (g^d)^q g^r = e^q g^r = g^r$. Since $g^r \neq e$ for $1 \leq r < d$ then we have $r = 0$ and therefore $m - n = qd$ so $d|(m-n)$.

(ii)

Lagrange's Theorem states that $|H|$ divides $|G|$.

(iii)

Let $H = \{e, g, g^2, \ldots, g^{d-1}\}$ be the cyclic subgroup generated by g. Using (i) we have that all the elements are distinct so $|H| = d$ and by (ii) we have that $|H|$ divides $|G|$. Thus d divides $|G|$. (QED)

Q3

(i)

$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$

(ii)

$h \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}$

(iii)

$h \circ f = (13)(245)(6) = (13)(245)$

(iv)

We need $(h \circ f)^m = (13)^m(245)^m = e$ hence m is the LCM of 2 and 3 so $m = 6$.

Q4

(i)

Let $g_1, g_2 \in N$ and fix $s \in S$. We have $g_2 s g_2^{-1} = s' \in S$ and $g_1 s' g_1^{-1} = s'' \in S$. Now observe that

$$\begin{aligned}(g_1g_2)s(g_1g_2)^{-1} &= g_1(g_2 s g_2^{-1})g_1^{-1} \\ &= g_1 s' g_1^{-1} \\ &= s'' \in S.\end{aligned}$$

Thus, $g_1g_2 \in N$ so N satisfies (S1).

Let $g \in N$ and define $f_g : S \to S$ by

$$f_g(s) = gsg^{-1}.$$

Note that f_g is well-defined since $g \in N$. Claim : f_g is bijective

Proof : Since G is finite, S is finite. Thus it suffices to prove that f_g is injective. Let $s_1, s_2 \in S$. Then

$$\begin{aligned}f_g(s_1) = f_g(s_2) &\implies gs_1g^{-1} = gs_2g^{-1} \\ &\implies s_1 = s_2.\end{aligned}$$

Now fix $s \in S$. By surjectivity of f_g, $\exists s' \in S$ such that $f_g(s') = s$. Then $gs'g^{-1} = s \implies g^{-1}sg = s' \in S$. Since the choice of s is arbitrary, we conclude that $\forall s \in S,\ g^{-1}sg \in S$. Thus $g^{-1} \in N$ so N satisfies (S2).

(ii)

If G is infinite, we can find a counterexample that does not satisfy (S2).
Counterexample: Let $(G,*) = (\mathrm{GL}(2,\mathbb{R}), \times)$ and let

$$S = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in G : x \geq 1 \right\}$$

Then $X = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in N$ because

$$X \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} X^{-1} = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix} \in S$$

for all $x \geq 1$. However, $X^{-1} = \begin{pmatrix} 2^{-1} & 0 \\ 0 & 1 \end{pmatrix} \notin N$ as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in S$ but

$$X \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} X^{-1} = \begin{pmatrix} 1 & 2^{-1} \\ 0 & 1 \end{pmatrix} \notin S.$$

Q5

(i)

Take $g_1, g_2 \in K$. Then $\phi(g_1) = \phi(g_2) = e_H$ and $\phi(g_2^{-1}) = (\phi(g_2))^{-1} = (e_H)^{-1} = e_H$. We have that $\phi(g_1 * g_2^{-1}) = \phi(g_1) * \phi(g_2)^{-1} = e_H * e_H = e_H$ so $g_1 * g_2^{-1} \in K$. Thus K is a subgroup by (S).

(ii)

Take $g \in G$ and $k \in K$. Then $\phi(gkg^{-1}) = \phi(g) * \phi(k) * \phi(g)^{-1} =$
$\phi(g) * e_H * \phi(g)^{-1} = \phi(g) * \phi(g)^{-1} = e_H$. Hence, $gkg^{-1} \in K$ and K is normal.

(iii)

Assume that $\phi(g_1) = \phi(g_2)$. Then $e_H = \phi(g_1) * \phi(g_2)^{-1} = \phi(g_1 g_2^{-1})$. We have $g_1 g_2^{-1} \in K = \{e_G\} \implies g_1 g_2^{-1} = e_G \implies g_1 = g_2$ so ϕ is injective.

Q6

Firstly, if $H = \{0\}$ then $H = 0\mathbb{Z}$. If $H \neq \{0\}$ then H contains a nonzero integer x and since it is a group, it contains $-x$ too, so it contains at least 1 positive integer, $|x|$. Let d be the smallest positive integer, then $0 < d \leq |x|$ and since H is a group, it contains $-d$ as well. For positive integer k, H contains kd and $-kd$ as well so $H \supseteq d\mathbb{Z}$, i.e. it contains all multiples of d.

Let $x \in H$ then by Euclidean Algorithm, $x = qd + r$, $0 \leq r < d$. But $qd \in H$ as all multiples of d are in H, so $r = x – qd = x + (-q)d \in H$. Noting that d was the smallest positive integer in H, $r = 0$ and therefore $x = qd \in d\mathbb{Z}$. Hence, $H \subseteq d\mathbb{Z}$. By both subset inclusions, $H = d\mathbb{Z}$.

Q7

(i)

If H is a subgroup that contains $20\mathbb{Z}$, by Q6, $H = d\mathbb{Z}$ where d is a nonzero integer. Since H contains 20, d must be a divisor of 20. Hence, $H = \mathbb{Z}, 2\mathbb{Z}, 4\mathbb{Z}, 5\mathbb{Z}, 10\mathbb{Z}, 20\mathbb{Z}$.

(ii)

Let $\phi\colon \mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$ be the quotient homomorphism which is a surjective group homomorphism. Hence, by the Fourth Isomorphism Theorem/Correspondence Theorem, there is a bijection between the set of subgroups of containing $20\mathbb{Z}$ and the set of subgroups of $\mathbb{Z}/20\mathbb{Z}$ so there are 6 such subgroups, as follows:

$$\begin{aligned}
\phi(\mathbb{Z}) &= \mathbb{Z}/20\mathbb{Z}, \\
\phi(2\mathbb{Z}) &= \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}, \\
\phi(4\mathbb{Z}) &= \{0, 4, 8, 12, 16\}, \\
\phi(5\mathbb{Z}) &= \{0, 5, 10, 15\}, \\
\phi(10\mathbb{Z}) &= \{0, 10\} \text{ and} \\
\phi(20\mathbb{Z}) &= \{0\}.
\end{aligned}$$

Q8

We show that $\mathrm{Aut}(G)$ satisfies (G1) to (G4) of the group axioms.

(G1) Let $\phi\colon G \to G$ and $\psi\colon G \to G$ be automorphisms in G. Since ϕ and ψ are bijections, $\phi \circ \psi$ is a bijection. For $x, y \in G$,

$$\begin{aligned}
\phi \circ \psi(x * y) &= \phi(\psi(x * y)) = \phi(\psi(x) * \psi(y)) = \phi(\psi(x)) * \phi(\psi(y)) \\
&= (\phi \circ \psi(x)) * (\phi \circ \psi(y)).
\end{aligned}$$

hence, $\phi \circ \psi$ is an isomorphism and $\phi \circ \psi \in \mathrm{Aut}(G)$
(G2) The composition of functions is associative.
(G3) Let $e\colon G \to G$ be the identity function. Then e is a bijection and $e(x * y) = x * y = e(x) * e(y)$ for $x, y \in G$ hence e is an isomorphism and $e \in \mathrm{Aut}(G)$. Also, for $\phi \in \mathrm{Aut}(G)$, $\phi \circ e = e \circ \phi = \phi$ so e is the identity element.
(G4) For $\phi \in G$, since ϕ is bijective, it's inverse ϕ^{-1} exists and is a bijection.
Take $x, y \in G$ and let $x' = \phi^{-1}(x)$, $y' = \phi^{-1}(y)$. Then $\phi(x') = x$ and $\phi(y') = y$. We have $\phi(x' * y') = \phi(x') * \phi(y') = x * y$ so $\phi^{-1}(x * y) = x' * y' = \phi^{-1}(x) * \phi^{-1}(y)$. Thus ϕ^{-1} is also an automorphism so $\phi^{-1} \in \mathrm{Aut}(G)$.

By (G1) to (G4), $\mathrm{Aut}(G)$ is a group.

Q9

(i)

Fix arbitrary $g \in G$ and define $\phi_g : G \to G$ by

$$\phi_g(x) = gxg^{-1}.$$

Then ϕ_g is an automorphism on G and since H is characteristic, $\phi_g(h) \in H \implies ghg^{-1} \in H$ so H is normal.

(ii)

Since $\phi \in \mathrm{Aut}(G)$ is a group isomorphism, then so is its inverse, by Q8. If H is the characteristic subgroup of G, $\rho(h) = \phi(h) \in H$ and $\rho^{-1}(h) = \phi^{-1}(h) \in H$ so the images of ρ and ρ^{-1} lie in H and we have $\rho\colon H \to H$ and $\rho^{-1}\colon H \to H$ so ρ is a bijection. Also, for $h_1, h_2 \in H$ we have $\rho(h_1 h_2) = \phi(h_1 h_2) = \phi(h_1) * \phi(h_2)$ so ρ is a group isomorphism.

(iii)

Let $\phi \in \mathrm{Aut}(G)$ and let ρ denote the function of ϕ restricted to H. By (ii), $\rho \in \mathrm{Aut}(H)$ and since K is a characteristic subgroup of H, $\forall k \in K,\ \rho(k) \in K$. Then $\forall k \in K,\ \phi(k) = \rho(k) \in K$ so K is characteristic in G.