MA2202 - Algebra I Suggested Solutions

(Semester 2, AY2022/2023)

Written by: Xu Xuezhou
Audited by: Clarence Chew Xuan Da
Typeset by: Chow Yong Lam

Question 1

(i) $d = \gcd(16287, 7031) = 89$. This is because:

$$\begin{aligned} 16287 &= 7032 \times 2 + 2225 \\ 7032 &= 2225 \times 3 + 356 \\ 2225 &= 356 \times 6 + 89 \\ 356 &= 89 \times 4 + 0 \end{aligned}$$

(ii)

$$\begin{aligned} d = 89 &= 2225 - 6 \times 356 \\ &= 2225 - 6 \times (7031 - 3 \times 2225) \\ &= 19 \times 2225 - 6 \times 7031 \\ &= 19 \times (16287 - 2 \times 7031) - 6 \times 7031 \\ &= 19 \times 16287 - 44 \times 7031 \end{aligned}$$

(iii) By (ii),

$$\begin{aligned} 19 \times 16287 - 44 \times 7031 &= d \\ (-2) \times 19 \times 16287 - (-2) \times 44 \times 7031 &= -2d \\ -38 \times 16287 + 88 \times 7031 &= -2d \\ 88 \times 7031 &= -2d (\text{mod } 16287) \end{aligned}$$

Thus, we found a solution $x = 88$.

Question 2

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 6 & 1 & 4 & 2 & 9 & 3 & 7 \end{pmatrix}$$

(i) By cyclic notation, $f = (154)(2836)(79)$.
(ii) $O(f) = 4 \times 3 = 12$.
(iii)$f = (154)(2836)(79) = (15)(54)(28)(83)(36)(79)$. f is a composition of six transpositions, so it is an even permutation.

Question 3

Let H be a subgroup of $(\mathbb{Z}, +)$. If $H = \{0\}$, then we set $d = 0$ and we are done.

Otherwise, H has a nonzero element x. Since H is a group, it contains $-x$ too. Hence, H contains at least one non-negative integer, namely $|x|$. Let d be the smallest positive integer in H, then $0 < d < |x|$.
Claim 1: $d\mathbb{Z} \subseteq H$.
Since H is a group, $-d \in H$. For a positive integer a, $ad \in H$ and $(-a)d \in H$. Hence, H contains all multiples of d, i.e., $d\mathbb{Z} \subseteq H$.
Claim 2: $H \subseteq d\mathbb{Z}$.
Let $x \in H$. By division algorithm, $x = qd + r$ where $0 \leq r < d$. Since $qd \in H$, $r = x - qd \in H$. This forces $r = 0$ so $x - qd = 0 \implies x = qd \in d\mathbb{Z}$.
In conclusion, $H = d\mathbb{Z}$.

Question 4

(i) Since $M \subseteq \mathbb{Z}/d\mathbb{Z}, h \in \mathbb{Z}/d\mathbb{Z}$ where h is the smallest positive integer in M. Suppose nh is the largest element in M, then $(n+1)h = 0 \in M$. $0 = (n+1)h \in M$. Therefore, h divides d.
(ii) By (i), $M = \{0, h, 2h, \cdots, nh\}$ and $(n+1)h = d$. Thus, $nh = d-h$, which makes $M = \{0, h, 2h, \cdots, d-h\}$

Question 5

Let $(G, *)$ be a cyclic group with generator g.
(i) Suppose G is an infinite group. Define $\phi : (G, *) \to (\mathbb{Z}, +)$, $\phi(g^n) = n$. Define $\varphi : (\mathbb{Z}, +) \to (G, *)$, $\varphi(n) = g^n$. Since $\phi \circ \varphi(n) = \phi(g^n) = n$ and $\varphi \circ \phi(g^n) = \varphi(n) = g^n$, ϕ is invertible. Also, let $g^a, g^b \in (G, *)$.

$$\phi(g^a * g^b) = \phi(g^{a+b}) = a + b = \phi(g^a) + \phi(g^b)$$

Thus, ϕ is homomorphic. Therefore, $(G, *)$ is isomorphic to $(\mathbb{Z}, +)$.
(ii) Suppose G is a finite group. Define $\phi : (G, *) \to (\mathbb{Z}/d\mathbb{Z}, +)$, $\phi(g^n) = n$. Define $\varphi : (\mathbb{Z}/d\mathbb{Z}, +) \to (G, *)$, $\varphi(n) = g^n$. Since $\phi \circ \varphi(n) = \phi(g^n) = n$ and $\varphi \circ \phi(g^n) = \varphi(n) = g^n$, ϕ is invertible. Also, let $g^a, g^b \in (G, *)$, and let d be the order of $(G, *)$.

$$\phi(g^a * g^b) = \phi(g^{a+b-kd}) = a + b - kd \in (\mathbb{Z}, +)$$

where $k = 0$ if $a + b < d$ and $k = 1$ otherwise. Thus, ϕ is homomorphic. Therefore, $(G, *)$ is isomorphic to $(\mathbb{Z}/d\mathbb{Z}, +)$.
(iii) Let M be a subgroup of G. If G is infinite, let H be a subgroup of $(\mathbb{Z}, +)$. By Question 3, there exists a non-negative integer d such that $H = d\mathbb{Z}$. Since G is isomorphic to $\mathbb{Z}$, M is isomorphic to H. Then, M is cyclic. Similarly, if G is finite, M is isomorphic to $\{0, h, 2h, \cdots, d-h\}$ which is cyclic.

Question 6

Let $(G, *)$ be a group. Given $x \in G$, define $S_x = \{gxg^{-1} \in G : g \in G\}, Z_x = \{g \in G : gx = xg\}$. The set S_x is called the *conjugacy class* of x and Z_x is called the *centralizer* of x.
(i) Suppose $y \in S_x$, then there exists $g \in G$ such that $y = gxg^{-1} \in G$.
Let $g' \in G$. Then $g'g \in G$ and:

$$g'y(g')^{-1} = g'gxg^{-1}(g')^{-1} = g'gx(g'g)^{-1} \in G \implies S_x \subseteq S_y.$$

On the other hand, $x = g^{-1}yg$ and:

$$g'x(g')^{-1} = g'g^{-1}yg(g')^{-1} = g'g^{-1}y(g'g^{-1})^{-1} \in S_x \implies S_y \subseteq S_x.$$

Hence, $S_x = S_y$.
(ii) Suppose $S_x \cap S_y$ is non-empty for some x and y in G. Let $z \in S_x \cap S_y$, then $z \in S_x$ and $z \in S_y$. By (i), $S_z = S_x = S_y$.
(iii) It is noted that $G = \cup_{x\in G} S_x$. From the previous two parts,

$$G = \bigsqcup_{x \in G} S_x$$

.

Question 7

Assume $(G, *)$ is a finite group.
(i) Let $g = e \in G$. Then $e \in Z_x$ and Z_x is not empty.
(ii) Since Z_x is non-empty, let $g_1, g_2 \in Z_x$. Then $g_1 x = x g_1, g_2 x = x g_2$. Since $(G, *)$ is finite, we only need to show $g_1 g_2 x = x g_1 g_2$.

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

Therefore, $g_1 g_2 \in Z_x$, and Z_x is a subgroup of G.
(iii) Consider G acting on G by conjugation. Then Z_x and S_x are the stabilizer and orbit of x respectively. By the Orbit-Stabilizer Theorem, the result follows.
(iv) The sum of the sizes of the disjoint S_x sets is 25. The size of S_e is 1. The size of S_x must be 1, 5 or 25. Take the sum among all the sizes, and consider modulo 5. If no such element exists, the total sum would be 1 modulo 5 which cannot be 25 (contradiction). Thus, such an element must exist.

Question 8

Let N be a normal subgroup of the symmetric group $(S_n, \circ)$ where $n \geq 5$. Let $M = N \cap A_n$ where A_n is the alternating group.
(i) M is non-empty since the identity is in both N and A_n. If $a, b \in M$, then ab^{-1} is in both N and A_n, and hence in M. Thus, M is a subgroup.
(ii) For $g \in A_n$, we have

$$gM = g(N \cap A_n) = gN \cap gA_n = Ng \cap A_n g = (N \cap A_n)g = Mg$$

. Since left cosets are right cosets, M is a normal subgroup in A_n.
(iii) Since A_n is simple for $n \geq 5$, it follows that $M = \{e\}$ or $M = A_n$.
If $M = A_n$, N contains A_n so N has index at most 2, so N is A_n or S_n.
Otherwise, $M = \{e\}$. N only has 1 even permutation. If N contains an odd permutation g, then $gg = e$ so g is of order 2, so it is a product of disjoint transpositions. If it is one transposition (a, b), then since N is normal, we can conjugate it to be (c, d), multiplying together forming $(a, b)(c, d) \neq e$. If it has at least two transpositions $(a, b)(c, d), \cdots$, then we can conjugate it to $h = (a, c)(b, d) \cdots$, where a, b, c, d are distinct, and $gh = (a, d)(b, c) \neq e$. Thus, N has no odd permutation so it follows that $N = M = \{e\}$.