Modern Algebra I — HW 4 Solutions

Problem 1 Note that the residue class $[1]$ of 1 modulo 7 is the multiplicative identity in $\mathbb{Z}_7^*$. All remaining elements can be written as powers of $[3]$:
$[3]^1 = [3]$, $[3]^2 = [9] = [2]$, $[3]^3 = [3][2] = [6]$, $[3]^4 = [2]^2 = [4]$, $[3]^5 = [3][4] = [12] = [5]$.
So, $\mathbb{Z}_7^*$ is a multiplicative cyclic group with generator $[3]$. □

Problem 2 (a) We know that every subgroup of a cyclic group is cyclic. Let H be a subgroup of $\mathbb{Z}_{81}$ generated by the residue class $[a]$. Then $|H|$ = order of $[a]$ in $\mathbb{Z}_{81}$ is one of the divisors of (81), namely $1, 3, 9, 27$ or 81. We also know that for every divisor of $|\mathbb{Z}_{81}| = 81$, there is a unique (cyclic) subgroup of $\mathbb{Z}_{81}$ of that order. Thus, the following are the only subgroups of $\mathbb{Z}_{81}$:

$\{[0]\}$ of order 1
$\{[0], [27], [54]\}$ of order 3
$\{[9m] \mid m \in \mathbb{Z}\}$ of order 9
$\{[3m] \mid m \in \mathbb{Z}\}$ of order 27
$\mathbb{Z}_{81}$ itself of order 81 □

(b) 12 is not a divisor of 42, so $\mathbb{Z}_{42}$ does not have any subgroup of order 12.
14 is a divisor of 42, so $\mathbb{Z}_{42}$ has a unique subgroup of order 14 →

$$\{[0], [3], [6], \dots, [39]\} = \{[3m] \mid m \in \mathbb{Z}\}$$ □

Problem 3 (a) $\forall g, h \in G$, we have $gh = g^{-1}h^{-1} = (g^{-1}h^{-1})^{-1} = (h^{-1})^{-1}(g^{-1})^{-1} = hg$. □

(b) Suppose that $g \neq g^{-1}$ for any $g \neq e$ in G. Then G, as a set, consists of e and pairs of elements g, g^{-1}. Then G has an odd number of elements. However, we know that the order of G is even. So, there must be some $g \neq e$ in G with $g = g^{-1}$ or $g^2 = gg^{-1} = e$. □

Problem 4 (a) We know that $e \in H$. If $h_1, h_2 \in H$, then $h_1 = g^{m_1}$, $h_2 = g^{m_2}$ for some integers m_1, m_2, and then $h_1 h_2 = g^{m_1+m_2} \in H$. Moreover, for any $h = g^m \in H$, we have $h^{-1} = g^{-m} \in H$. So, by definition, H is a subgroup of G. It's clear that H is cyclic with generator g. $\square$

(b) Let H be a cyclic subgroup of G. Then H is generated (as a cyclic group) by some element $g \in H \subseteq G$. Then $H = \langle g \rangle$ for this $g \in G$. $\square$

Problem 5 (Notation from Week 3 slides) We know that D_{26} has

$$\underbrace{e}_{\text{identity}},\ \underbrace{s, s^2, \ldots, s^{12}}_{\substack{\text{rotations} \\ s^{13}=e}},\ \underbrace{f, fs, fs^2, \ldots, fs^{12}}_{\substack{\text{reflections} \\ (fs^i)^2 = e}}$$

Then D_{26} has the following subgroups $\to$

$\{e\}$ cyclic with generator e

$\{e, s, s^2, \ldots, s^{12}\}$ cyclic with generator s

$\{e, fs^i\}$ for any $0 \leq i \leq 12$ cyclic with generator fs^i

D_{26} not cyclic

We can show that these are the only subgroups of D_{26}.

Let H be a subgroup of D_{26}.

Case 1: $s^i \in H$ for some $1 \leq i \leq 12$. Since the order of s is a prime number (13), any s^i can generate $\langle s \rangle$ and $\{e, s, s^2, \ldots, s^{12}\} \subseteq H$. Now if some fs^j is in H, then so is the product $(fs^j \cdot s^{13-j}) s^k = fs^k$ for any k, and $H = D_{26}$. If no fs^j is in H, then $H = \langle s \rangle$.

Case 2: No power of s, other than e, lies in H. Unless $H = \{e\}$, some $fs^i \in H$. If another $fs^j \in H$, then

$$fs^i fs^j = s^{-i} ff s^j = s^{j-i} \in H.$$

Then s^{j-i} must be e and $s^j = s^i$. So, H is simply $\{e, fs^i\}$. $\square$

Problem 6 (a) $G\times H$ has the multiplicative identity $(e_G, e_H) \rightarrow$

$$(e_G, e_H)(g,h) = (e_G g, e_H h) = (g,h)$$
$$(g,h)(e_G, e_H) = (g e_G, h e_H) = (g,h)$$

for any $(g,h) \in G\times H$.

The multiplication in $G\times H$ is associative $\rightarrow$

$$\begin{aligned}((g_1,h_1)(g_2,h_2))(g_3,h_3) &= (g_1g_2, h_1h_2)(g_3,h_3)\\ &= ((g_1g_2)g_3, (h_1h_2)h_3)\\ \text{By associativity in } G, H \rightarrow &= (g_1(g_2g_3), h_1(h_2h_3))\\ &= (g_1,h_1)((g_2,h_2)(g_3h_3))\end{aligned}$$

Finally, every $(g,h) \in G\times H$ has an inverse $\rightarrow$

$$(g,h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H)$$
$$(g^{-1}, h^{-1})(g,h) = (g^{-1}g, h^{-1}h) = (e_G, e_H)$$

inverse in G inverse in H

$\square$

(b) • Consider $([1]_3, [1]_7) \in \mathbb{Z}_3 \times \mathbb{Z}_7$. Let n be the order of this element. Then

$$n([1]_3, [1]_7) = ([n]_3, [n]_7) = ([0]_3, [0]_7).$$

This means that n is divisible by both 3 and 7. Then n must be divisible by 21. However, $n \le |\mathbb{Z}_3 \times \mathbb{Z}_7| = 21$. So, $n = 21$ and

$$m([1]_3, [1]_7) \quad \text{with} \quad 0 \le m \le 20$$

must be distinct 21 elements of $\mathbb{Z}_3 \times \mathbb{Z}_7$. Thus, $\mathbb{Z}_3 \times \mathbb{Z}_7$ is the cyclic group generated by $([1]_3, [1]_7)$.

• Note that $5([a]_5, [b]_5) = ([0]_5, [0]_5) =$ identity in $\mathbb{Z}_5 \times \mathbb{Z}_5$ for any a, b. But $|\mathbb{Z}_5 \times \mathbb{Z}_5| = 25 > 5$. No element of $\mathbb{Z}_5 \times \mathbb{Z}_5$ can generate the entire group.

- $\mathbb{Z}_3 \times \mathbb{Z}_3$ has the following cyclic subgroups:

  $\{e\} = \{([0],[0])\}$,

  $\{e, ([0],[1]), ([0],[2])\}$, $\{e, ([1],[0]), ([2],[0])\}$,

  $\{e, ([1],[1]), ([2],[2])\}$, $\{e, ([2],[1]), ([1],[2])\}$.

  The 3-element subgroups can be generated by either of the non-identity elements in them.

$\square$